SAPIDO
Share the Joy

User Manual V 1.0

1

Table of Contents

Table of Contents 2
Chapter 1 Introduction 7
1.1 Hardware Features 7
1.2 Product Appearance 8
Chapter 2 System and Network Setup 10
2.1 Build Network Connection 10
2.1.1 Router Mode 10
2.1.2 AP Mode 11
2.1.3 Wi-Fi AP Mode 11
2.2 Connecting GR-1736 11
2.3 Network setup 12
2.3.1 Windows 2000 12
2.3.2 Windows XP 13
2.3.3 Windows Vista / Windows 7 14
2.4 Router IP Address Lookup 16
2.4.1 Log into Web GUI 17
Chapter 3 Internet Connection 19
3.1 Plug and Play 19
3.1.1 Smart Phone /iPhone Internet sharing plug and play 19
3.2 Router Mode- Using as a broadband router 21
3.2.1 One button setup 21
3.2.2 Parental Control 22
3.2.2.1 URL Filtering 22
3.2.2.2 Mac Filter Schedule 23
3.2.2.3 Schedule 24
3.2.3 AirCloud Storage 25
3.2.3.1 FTP server 25
3.2.3.2 Samba management 26
3.2.4 WAN Interface- Ethernet Port 26
3.2.4.1 Static IP 27
3.2.4.2 DHCP Client 29
3.2.4.3 PPPoE 30
3.2.4.4 PPTP 32
3.2.4.5 L2TP 33
3.2.4.6 Advance function 34
3.2.5 WAN Interface- 3G USB dongle 35
3.2.6 WAN Interface- Wireless 37

3.3 AP Mode-Using as a Access Point 38
3.4 WiFi AP Mode- Using as a Network Converter 40
Chapter 4 Wireless Setup 42
4.1 Wireless Setup 42
4.1.1 Setup Wireless LAN by WPS button 42
4.1.2 Wireless Basic Setup from Web GUI 44
4.1.2.1 Multiple APs 46
4.1.2.2 Enable Universal Repeater Mode 47
4.2 Wireless Security Setup 48
4.3 Wireless Access Control 50
Chapter 5 Router Mode Security Setup 52
5.1 NAT 52
5.1.1 Virtual Server 52
5.1.2 DMZ 53
5.2 Firewall 54
5.2.1 QoS 55
5.2.2 Port Filtering 56
5.2.3 IP Filtering 57
5.2.4 Denial of Service 58
5.2.5 VLAN Settings 59
5.3 Server Setup 60
5.3.1 Webcam server 60
Chapter 6 Advanced Setup 62
6.1 Dynamic DNS Setting Router 62
6.2 Wireless Advanced Setup 63
6.2.1 Wireless Site Survey WiFi-AP 65
6.2.2 WPS Router AP 65
6.3 System Management 67
6.3.1 Statistics 68
6.3.2 Change Password 69
6.3.3 Firmware Upgrade 69
6.3.4 Profile Save 70
6.3.5 Remote Manager 73
6.3.6 Time Zone Setting 73
6.3.7 UPnP Setting 74
6.3.8 VPN Passthrough Setting 75
6.3.9 Language Setting 76
6.3.10 Routing Setup 77

6.3.11 User Account Settings 79
6.3.12 Walk on LAN Schedule 79
6.4 Log & Status 80
6.4.1 Network Config 81
6.4.2 Event Log 83
6.5 Logout 84
Chapter 7 Samba Server 85
7.1 How to use GR-1736 as a Samba server 85
7.2 Air play 86
7.3 Printer Server 87
Chapter 8 DDNS Service Application 89
Chapter 9 Q & A 94
9.1 Installation 94
9.2 LED 94
9.3 IP Address 94
9.4 OS Setting 95
9.5 GR-1736 Setup 97
9.6 Wireless LAN 98
9.7 Support 100
9.8 Others 101
9.9 USB Device 101
Chapter 10 Appendices 102
10.1 Operating Systems 102
10.2 Browsers 102
10.3 Communications Regulation Information 102

FCC Statement

Federal Communication Commission Interference Statement This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

1. The device complies with Part 15 of the FCC rules. Operation is subject to the following conditions:
2. This device may not cause harmful interference, and this device must accept any interference received, including interference that may cause undesired operation.
3. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
4. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
5. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance20cm between the radiator & your body.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

Frequency range - 2400.0 - 2483.5 MHz

Country	Country	Reason/remark
Bulgaria	none	General authorization required for outdoor use and public service.
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012.
Italy	none	If used outside of own premises, general authorization is required.
Luxembourg	none	General authorization required for network and service supply (not for spectrum).
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund.
Russian Federation	none	Only for indoor applications.

Note: Please don't use the product outdoors in France

CE Statement of Conformity

Our product has been tested in typical configuration by Ecom Sertech Corp and was found to comply with the essential requirement of "Council Directive on the Approximation of the Laws of the Member Sates relating to Electromagnetic Compatibility" (89/336/EEC; 92/31/EEC; 93/68/EEC). The Declaration of Conformity can be found at the Sapido regional website. www.sapidotech.de

CE Information of Disposal

The electric and electronic equipment or unit which is labeled with crossed-out wheeled bin may not be disposed of with household waste. This mark is based on European Directive 2002/96/EC (for Waste Electric and Electronic Equipment=WEEE).

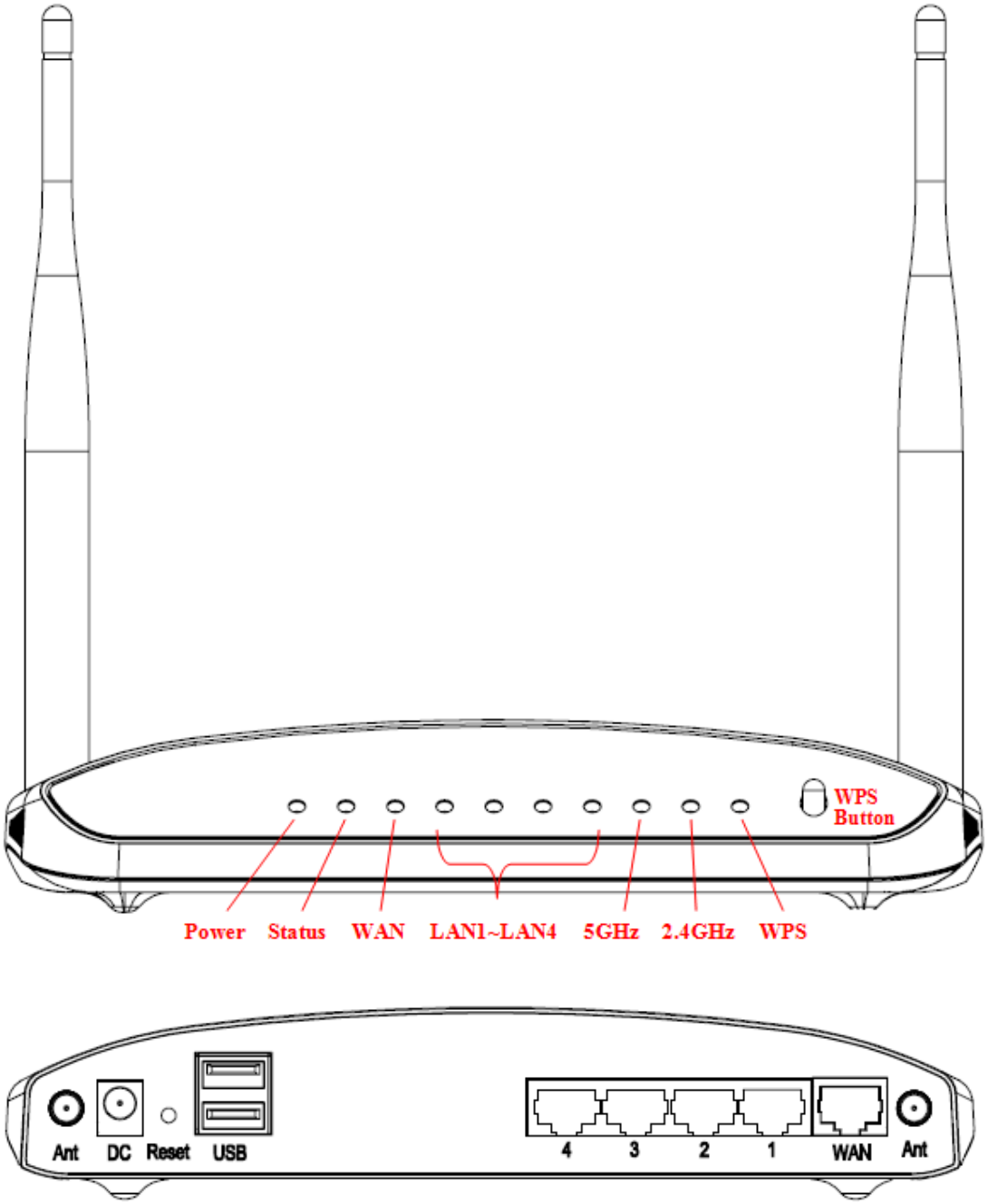
Please take it to the designated collection facilities. We will ensure the proper recycling, reuse and other forms of recovery of WEEE. WEEE has the potential effects on the environment and human health as a result of the presence of hazardous substances. You can contribute to eliminate these effects by your cooperation.

Chapter 1 Introduction

1.1 Hardware Features

Item	Specification
Key Components	
Main Processor	Realtek RTL8198 (600MHz)
Flash	8Mbytes Serial Flash
RAM	64Mbytes DDR2
Wireless Chip	Realtek RTL8192CE 2.4G 2T2R Realtek RTL8192DR 2.4G/5GHz dual-band 2T2R
Communication Interfaces	
WAN Port	1 x 10/100/1000Mbps RJ45 with auto MDI/MDIX
LAN Port	4 x 10/100/1000Mbps RJ45 with auto MDI/MDIX
USB Port	USB 2.0 host port x2
Wireless	IEEE 802.11a/ b/g/n 5G/2.4GHz concurrent 300+300Mbps
Others	
Wireless Antenna	External 5dBi x2
Transmission Power	802.11a: 16±2dBm @ normal temp. range 802.11b: 19±2dBm @ normal temp. range 802.11g: 16±2dBm @ normal temp. range 802.11n (2.4GHz): 14±2dBm @ normal temp. range 802.11n (5GHz): 21±1dBm @ normal temp. range
Receive Sensitivity	802.11a: TYP. -70dBm @ 10% PER 802.11b : TYP. -83dBm @ 8% PER 802.11g: TYP. -70dBm @ 10% PER 802.11n: TYP. -61dBm @ 10% PER
Button	**Reboot button / Reset button** – 1sec is for reboot ; 10 secs is for reset to default configuration **WPS button – WPS connection**
Operation Requirement	Operating Temp. 0 to 40℃ Storage Temp. -20 to 70℃ Operating Humidity 10% to 85% Non-Condensing Storage Humidity 5% to 90% Non-Condensing
Power Supply	Power Adapter DC12V/2A

1.2 Product Appearance



LED Indicator Status Description:

LED	Function	Color	Status	Description
Power	System status	Green	On	System is ready to work.
			Blinking 120ms	1. Power is being applied and system boot in progress. 2. Reset or firmware upgrade in progress.
WPS	WPS status	Green	Blinking 120ms	WPS function in progress.
2.4GHz	Wireless activity	Green	Blinking 30ms	Wireless Tx/Rx activity for 2.4GHz band.
5GHz	Wireless activity	Green	Blinking 30ms	Wireless Tx/Rx activity for 5GHz band.
WAN x 1	WAN port activity	Green	On	1000Mbps Ethernet is connected.
			Blinking 30ms	1000Mbps Ethernet Tx/Rx activity.
		Green	On	10/100Mbps Ethernet is connected.
			Blinking 120ms	10/100Mbps Ethernet Tx/Rx activity.
LAN x 4	LAN port activity	Green	On	1000Mbps Ethernet is connected.
			Blinking 30ms	1000Mbps Ethernet Tx/Rx activity.
		Green	On	10/100Mbps Ethernet is connected.
			Blinking 120ms	10/100Mbps Ethernet Tx/Rx activity.

Confidential

Chapter 2 System and Network Setup

The GR-1736 is an easy to setup and wireless device for various application and environment, especially for large installs such as hotels, offices space, warehouses, hot-spots and more.

To begin with GR-1736, you must have the following minimum system requirements. If your system can't correspond to the following requirements, you might get some unknown troubles on your system.

- λ Internet Account for XDSL/Cable Modem, or 3G.
- λ One Ethernet (10/100/1000 mbps) network interface card.
- λ TCP/IP and at least one web browser software installed (E.g.: Internet Explorer 6.0, Netscape Navigator 7.x, Apple Safari 2.03 or higher version).
- λ At lease one 802.11g (54Mbps) or one 802.11b (11Mbps) wireless adapter for wireless mobile clients.
- λ Recommended OS: WinXP, Visata or Win7 / Linux.

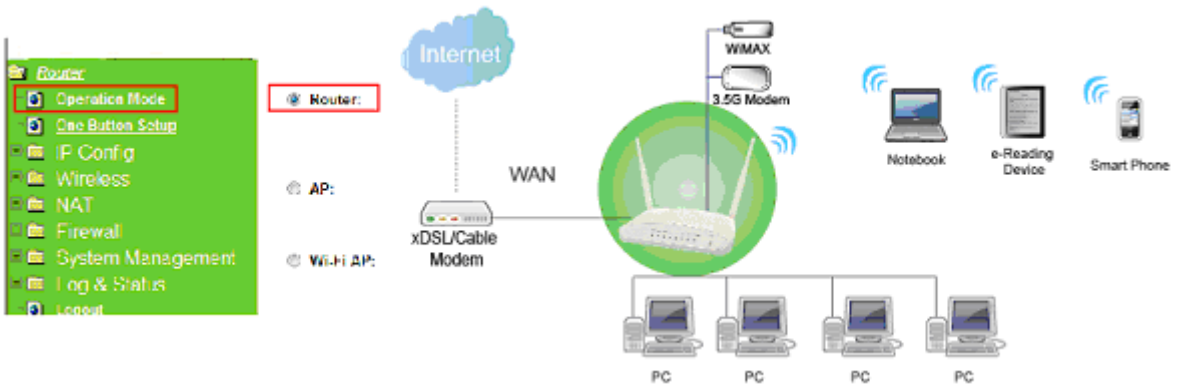
2.1 Build Network Connection

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.

Please confirm the network environment or the purpose before setting this product.

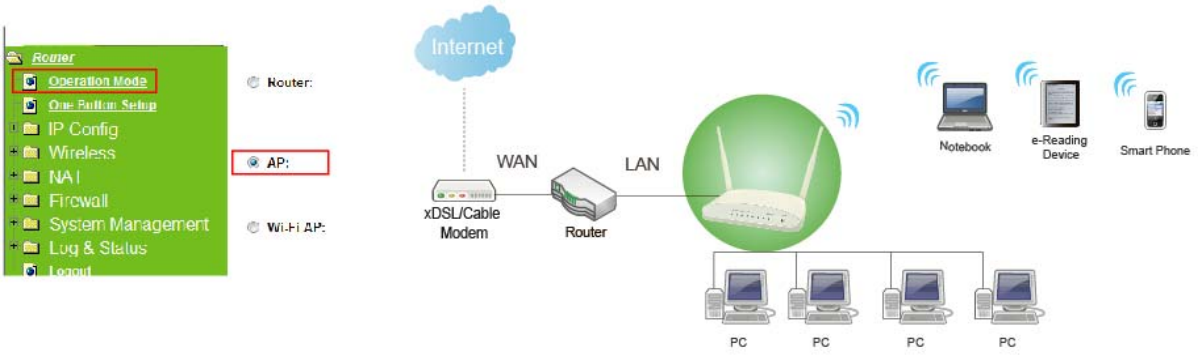
2.1.1 Router Mode

Switch to router mode through web GUI when the first setup.



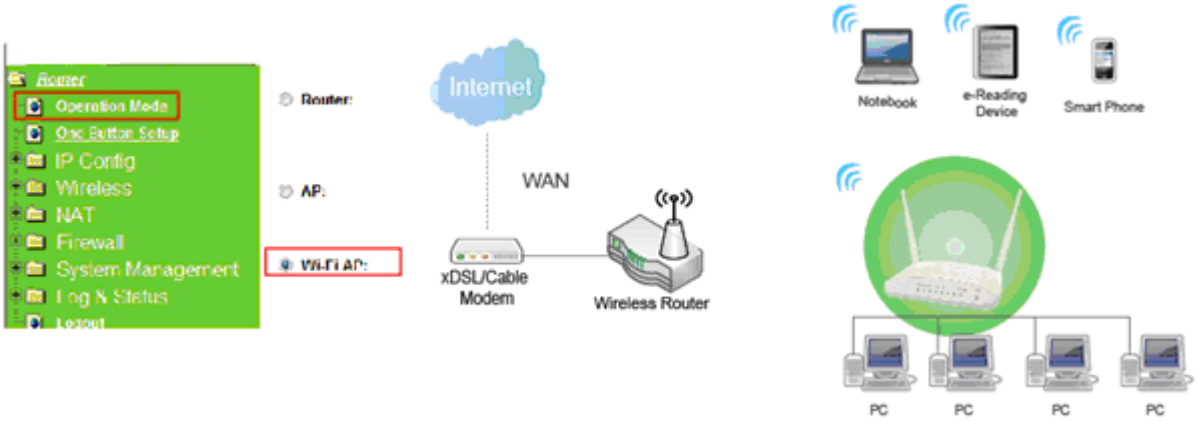
2.1.2 AP Mode

Switch to AP mode, if a router is already set at the house, and you want to make the wireless LAN communication.



2.1.3 Wi-Fi AP Mode

Switch to WiFi AP Mode when you connect to the internet wirelessly through PC and wireless device without wireless LAN function equipped.



2.2 Connecting GR-1736

Prepare the followings before the connection:

λ PC or Notebook for setup

λ Ethernet cable or 3G modem

1. Make sure you are under “Router Mode”.
2. Connect GR-1736 to xDSL/ Cable modem with the Ethernet cable, WAN to LAN.
3. Turn on your Computer.

2.3 Network setup

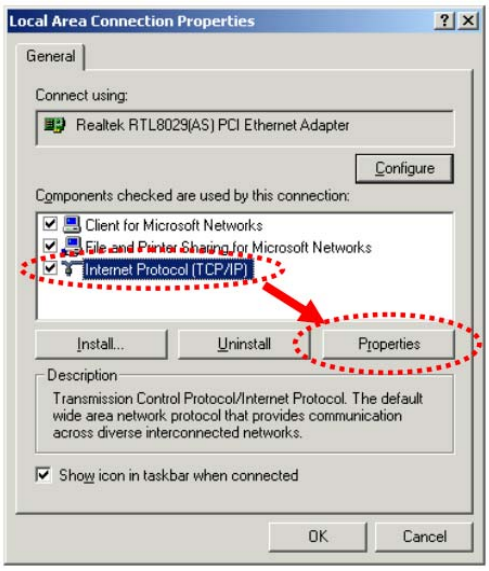
After the network connection is built, the next step is setup the router with proper network parameters, so it can work properly in your network environment. Before you connect to the wireless router and start configuration procedures, your computer must be able to get an IP address from the wireless router automatically (use dynamic IP address). If it’s set to use static IP address, or you’re unsure, please follow the below instructions to configure your computer with dynamic IP address:

If the operating system of your computer is….

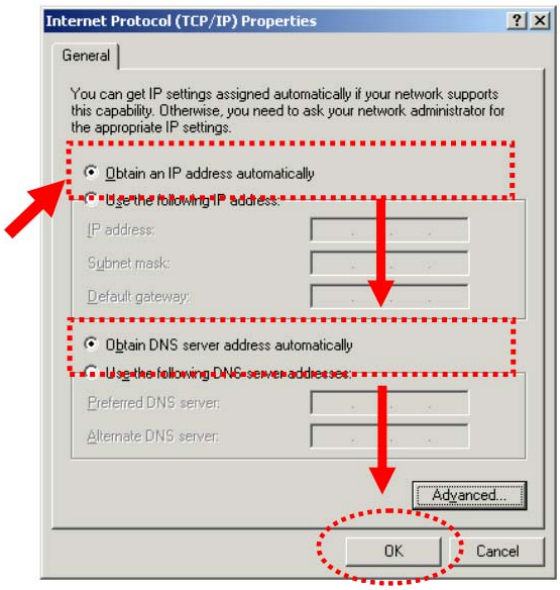
Windows 2000 - please go to section 2.3.1
Windows XP - please go to section 2.3.2
Windows Vista/Win7 - please go to section 2.3.3

2.3.1 Windows 2000

Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Double-click Network and Dial-up Connections icon, double click Local Area Connection, and Local Area Connection Properties window will appear. Select “Internet Protocol (TCP/IP)”, then click “Properties”.

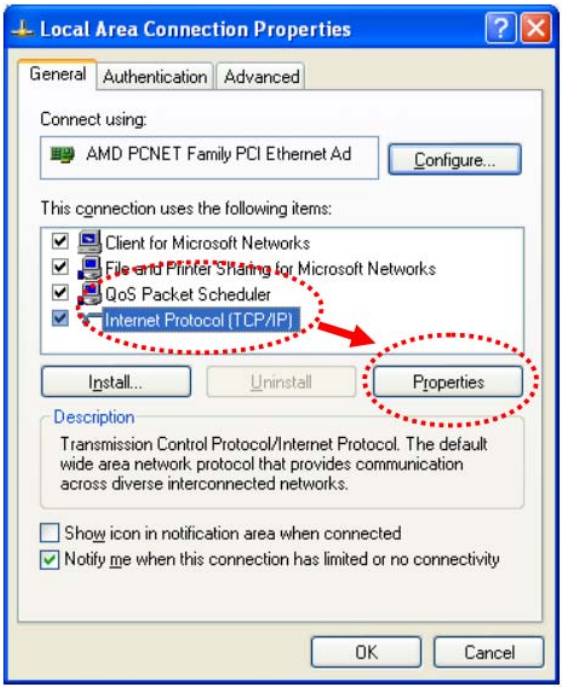


1. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.

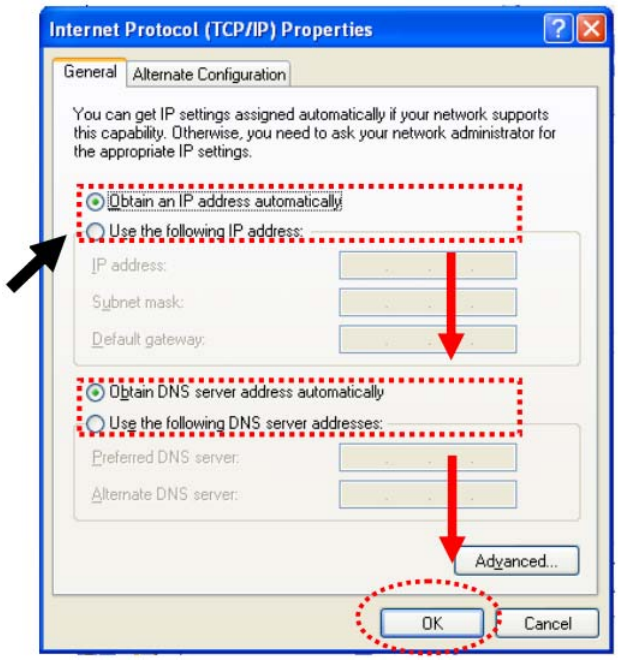

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2.3.2 Windows XP

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Double-click Network and Internet Connections icon, click Network Connections, then double-click Local Area Connection, Local Area Connection Status window will appear, and then click “Properties”.



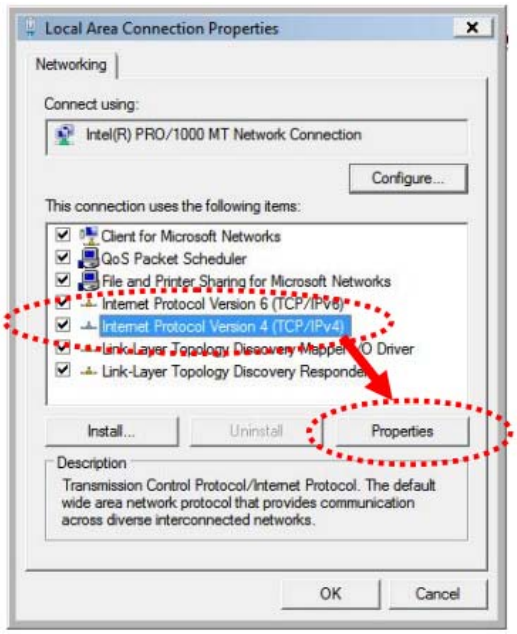
2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

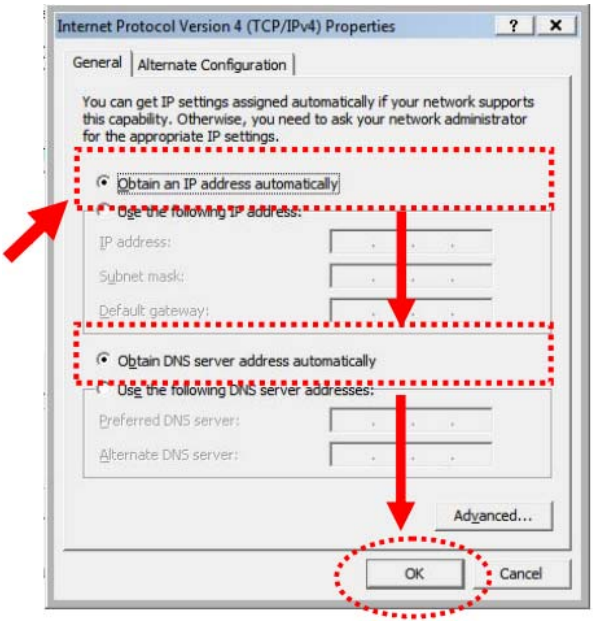
2.3.3 Windows Vista / Windows 7

1. Click “Start” button (it should be located at lower-left corner of your computer), then click control panel. Click View Network Status and Tasks, and then click Manage Network Connections. Right-click Local Area Network, then select “Properties”. Local Area

Connection Properties window will appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.



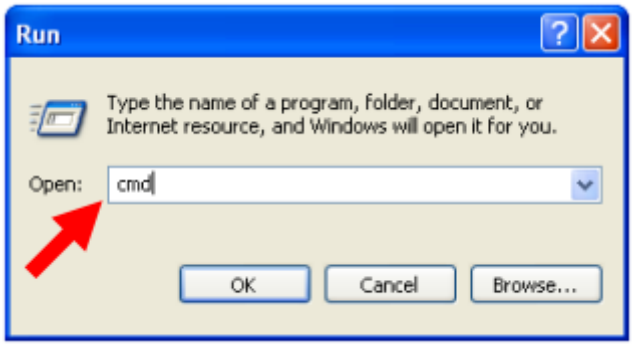
2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2.4 Router IP Address Lookup

After the IP address setup was completed, please clicks “start” → “run” at the bottom-lower corner of your desktop:

Input “cmd”, and then click “OK”.



Input “ipconfig”, then press “Enter” key. Please check the IP address followed by “Default Gateway” (In this example, the gateway IP address of router is 192.168.1.1)

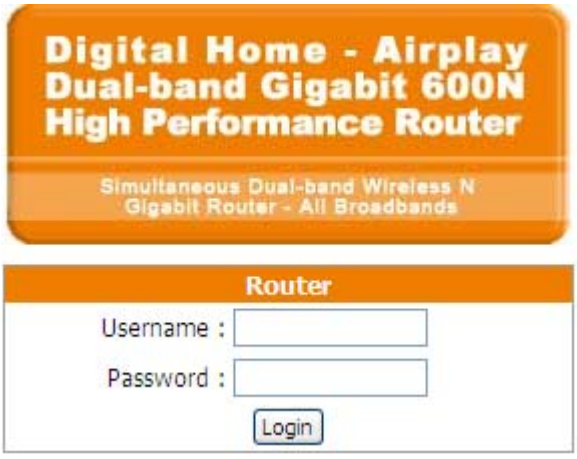
C:\Documents and Settings\demo>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\demo>

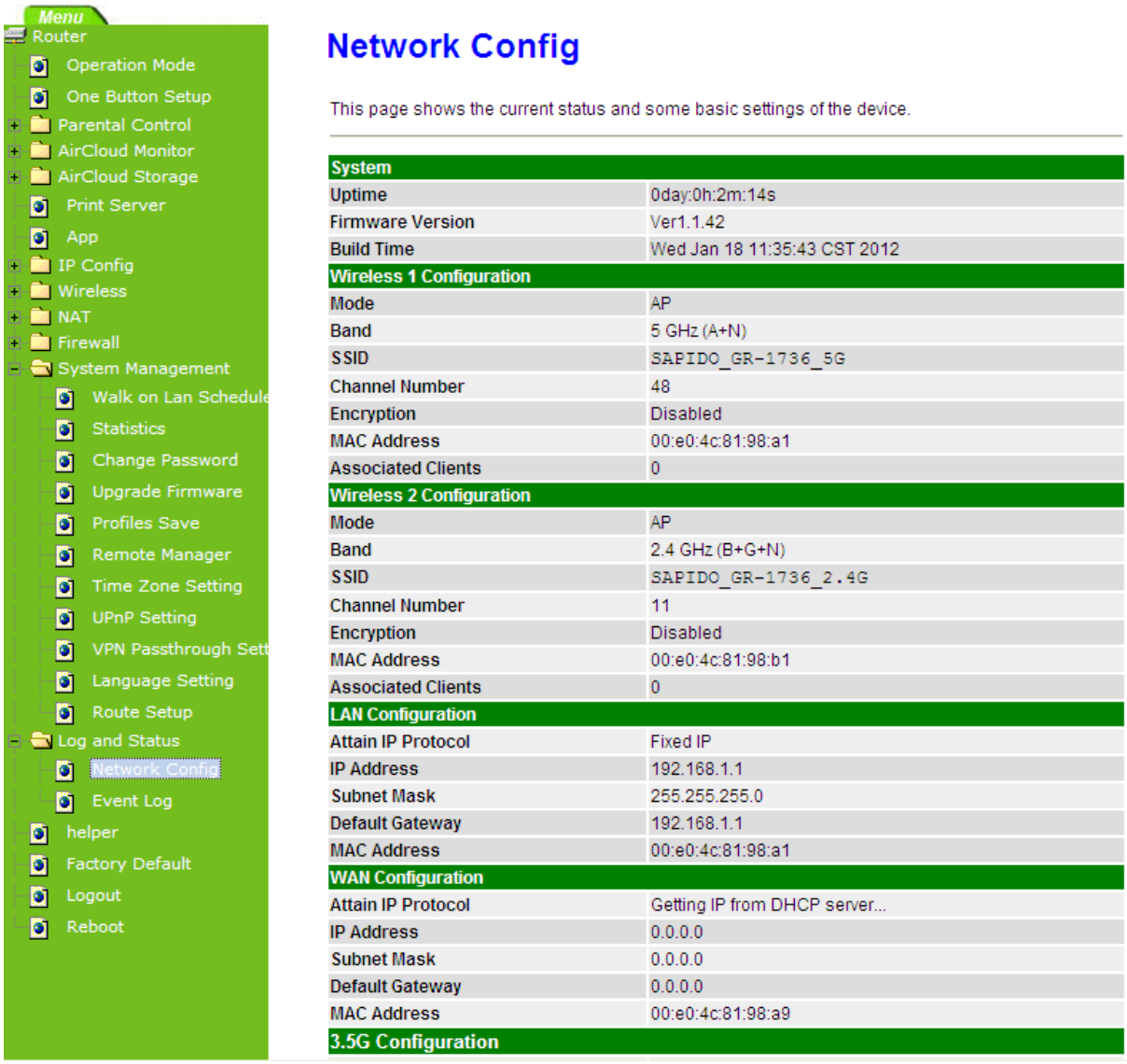
NOTE: If the IP address of Gateway is not displayed, or the address followed by 'IP Address' begins with "169.x.x.x", please recheck network connection between your computer and router, and / or go to the beginning of this chapter, to recheck every step of network setup procedure.

2.4.1 Log into Web GUI

After your computer obtained an IP address from wireless router, please start your web browser, and input the IP address of the wireless router in address bar, and the following message should be shown. Please click "admin" to login the GR-1736.

Enter the User name and Password in to the blank and then Click **Login**. The default values for User Name and Password are **admin** (all in lowercase letters).




Menu
Router
Operation Mode
One Button Setup
Parental Control
AirCloud Monitor
AirCloud Storage
Print Server
App
IP Config
Wireless
NAT
Firewall
System Management
Walk on Lan Schedule
Statistics
Change Password
Upgrade Firmware
Profiles Save
Remote Manager
Time Zone Setting
UPnP Setting
VPN Passthrough Sett
Language Setting
Route Setup
Log and Status
Event Log
helper
Factory Default
Logout
Reboot
Network Config
This page shows the current status and some basic settings of the device.
System
Uptime 0day:0h:2m:14s
Firmware Version Ver1.1.42
Build Time Wed Jan 18 11:35:43 CST 2012
Wireless 1 Configuration
Mode AP
Band 5 GHz (A+N)
SSID SAPIDO_GR-1736_5G
Channel Number 48
Encryption Disabled
MAC Address 00:e0:4c:81:98:a1
Associated Clients 0
Wireless 2 Configuration
Mode AP
Band 2.4 GHz (B+G+N)
SSID SAPIDO_GR-1736_2.4G
Channel Number 11
Encryption Disabled
MAC Address 00:e0:4c:81:98:b1
Associated Clients 0
LAN Configuration
Attain IP Protocol Fixed IP
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
MAC Address 00:e0:4c:81:98:a1
WAN Configuration
Attain IP Protocol Getting IP from DHCP server...
IP Address 0.0.0.0
Subnet Mask 0.0.0.0
Default Gateway 0.0.0.0
MAC Address 00:e0:4c:81:98:a9
3.5G Configuration

Chapter 3 Internet Connection

This Chapter describes how to setup GR-1736 to the internet. The GR-1736 is delivered with the following factory default parameters.

Default IP address: 192.168.1.1 (Router Mode)

192.168.1.254 (AP Mode)

192.168.1.254 (WiFi AP Mode)

Default IP subnet mask: 255.255.255.0

Web login user name: admin

Web login password: admin

3.1 Plug and Play

The GR-1736 supports four types of Internet connection method: 3G modem card, wire or wireless connection via xDSL/Cable modem. Just connect the 3G modem card or Ethernet cable to GR-1736, the router will recognize it automatically.

3.1.1 Smart Phone /iPhone Internet sharing plug and play

With GR-1736, you can build an instant 802.11n wireless broadband sharing environment with your iPhone, Windows Mobile or Google smart phone. During the time you can still answer calls, send SMS and charge your phone.

Step 1. Connect iPhone/Smart phone with GR-1736 via USB cable.

Step 2. Select “USB Tethering” as connection type.

Step 3. Click on “Done”.

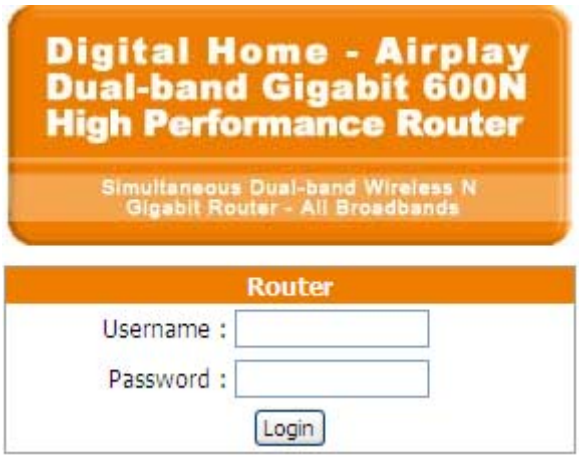
Step 4. Wait few seconds for pairing. When WAN LED on, the Internet is ready to access.

Note: 1. iPhone:
(1) Due to difference in 3G service bundled in various carriers, please check your 3G service supports Internet tethering.
(2) Enable Internet Tethering on iPhone 3GS / iPhone 4, and set up the screen lock to never to prevent the sharing is interrupted unexpected by the iPhone screen lock feature.
2. Google Android Phone: please turn on "USB modem mode” when connecting router.
3. Window Mobile Phone: please enable “USB to PC” function.

3.2 Router Mode- Using as a broadband router

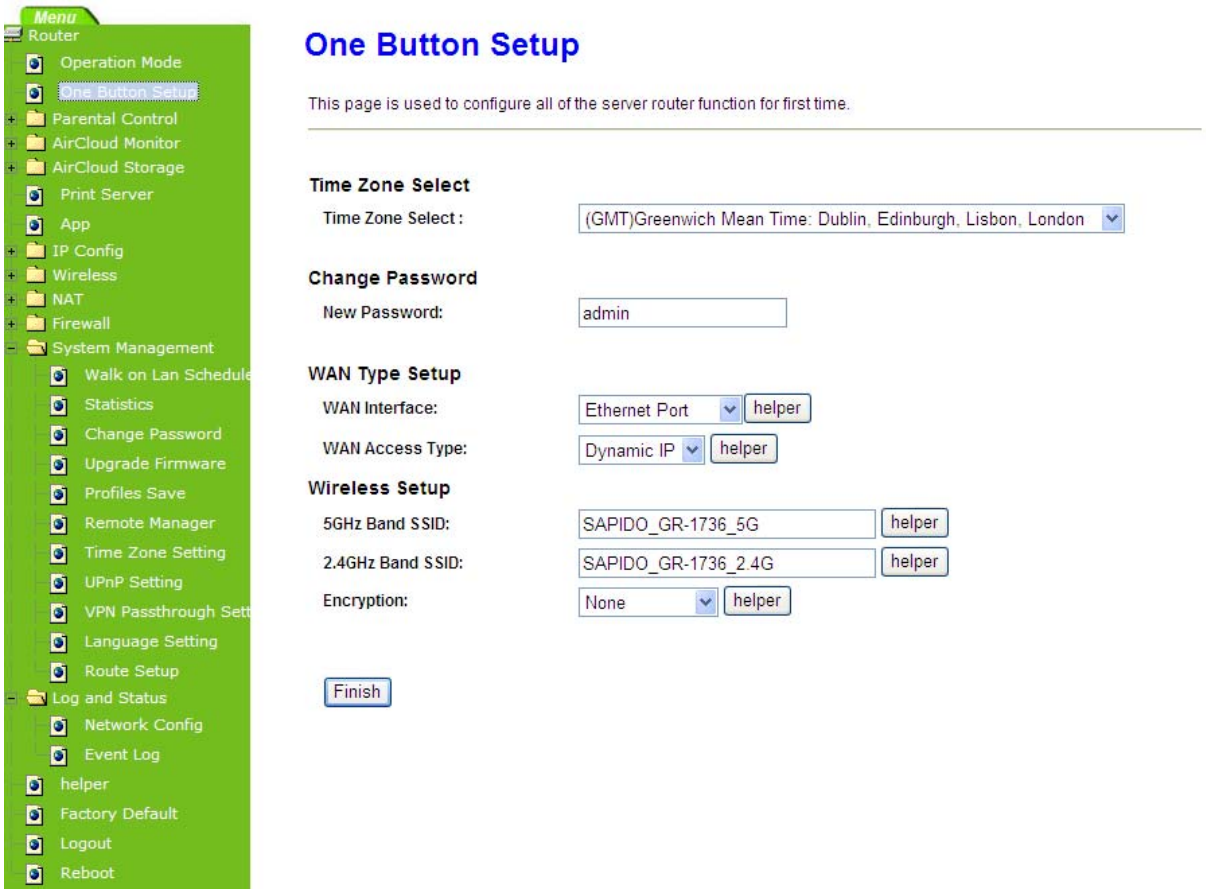
1. Open a Web browser, and enter http://192.168.1.1 (Default Gateway) into the blank.

2. Enter the User name and Password into the blank and then click **Login**. The default values for User Name and Password are **admin** (all in lowercase letters).



3.2.1 One button setup

This page is used to configure all of the server router function.

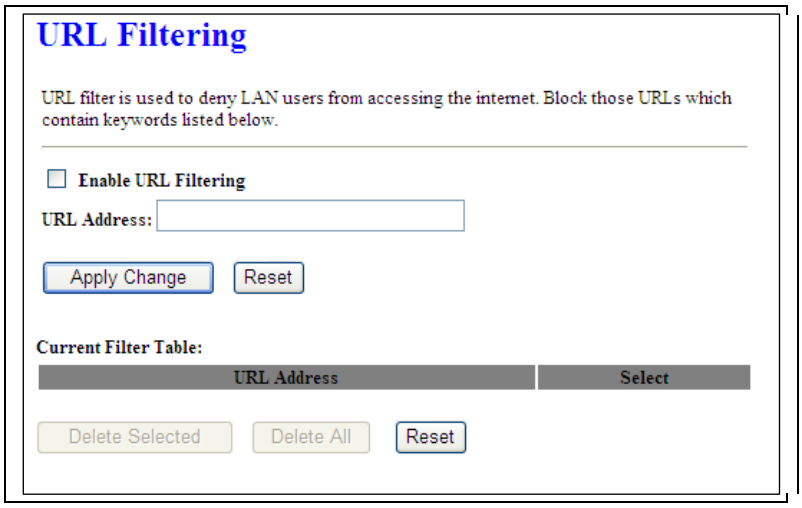


Item	Description
Time Zone Select	Select different time zone
Change Password	Set a new password
WAN Type Setup	There are several different WAN interface，Ethernet port、3.5G usb dongle、wireless
Wireless Setup	BR485d support 2.4GHz and 5GHz band
Encryption	Input DNS information which is provided by your ISP

3.2.2 Parental Control

3.2.2.1 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet

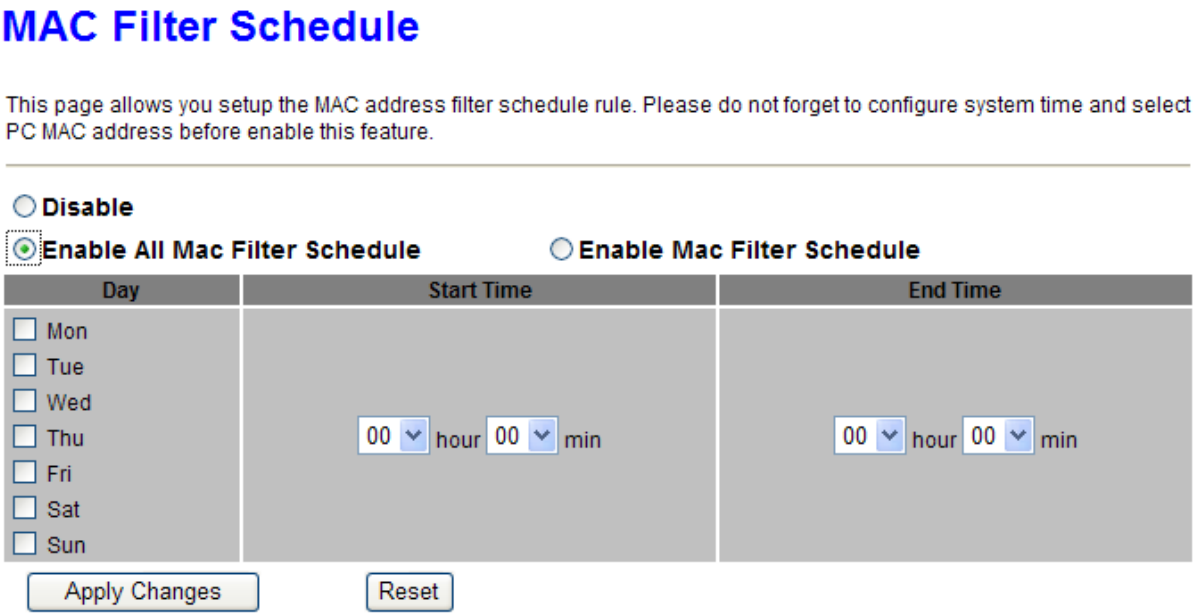


Item	Description
Enable URL Filtering	Please select Enable MAC Filtering to filter MAC addresses
URL Address	Please enter the MAC address that needs to be filtered.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

Notes: This function will not be in effect when the Virtual Server is enabled. Please disable Virtual Server before activate the URL Filtering function.

3.2.2.2 Mac Filter Schedule

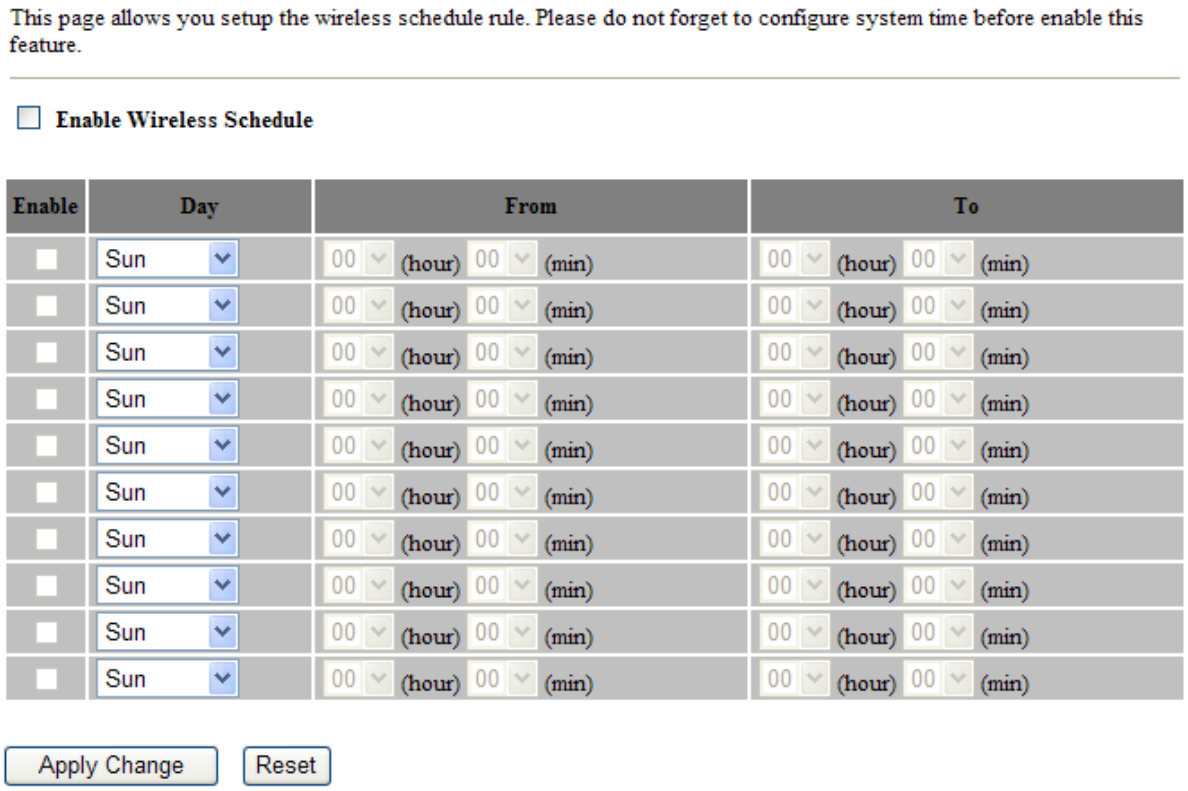
When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.



Item	Description
Enable MAC Filtering	Please select Enable MAC Filtering to filter MAC addresses.
MAC Address	Please enter the MAC address that needs to be filtered.
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

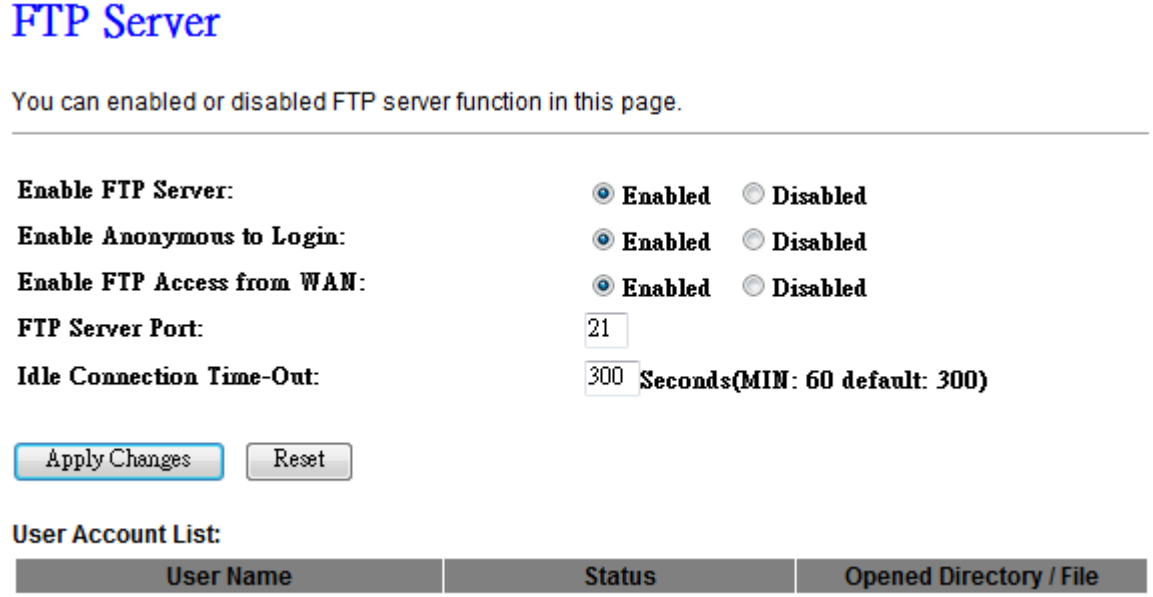
3.2.2.3 Schedule

Wireless available schedule



3.2.3 AirCloud Storage

3.2.3.1 FTP server


FTP Server
You can enabled or disabled FTP server function in this page.
Enable FTP Server: Enabled Disabled
Enable Anonymous to Login: Enabled Disabled
Enable FTP Access from WAN: Enabled Disabled
FTP Server Port: 21
Idle Connection Time-Out: 300 Seconds(MIN: 60 default: 300)
Apply Changes
Reset
User Account List:
User Name
Status
Opened Directory / File

Item	Description
Enable FTP Server	FTP server start or stop
Enable Anonymous to Login	Agree anonymous account login to FTP server

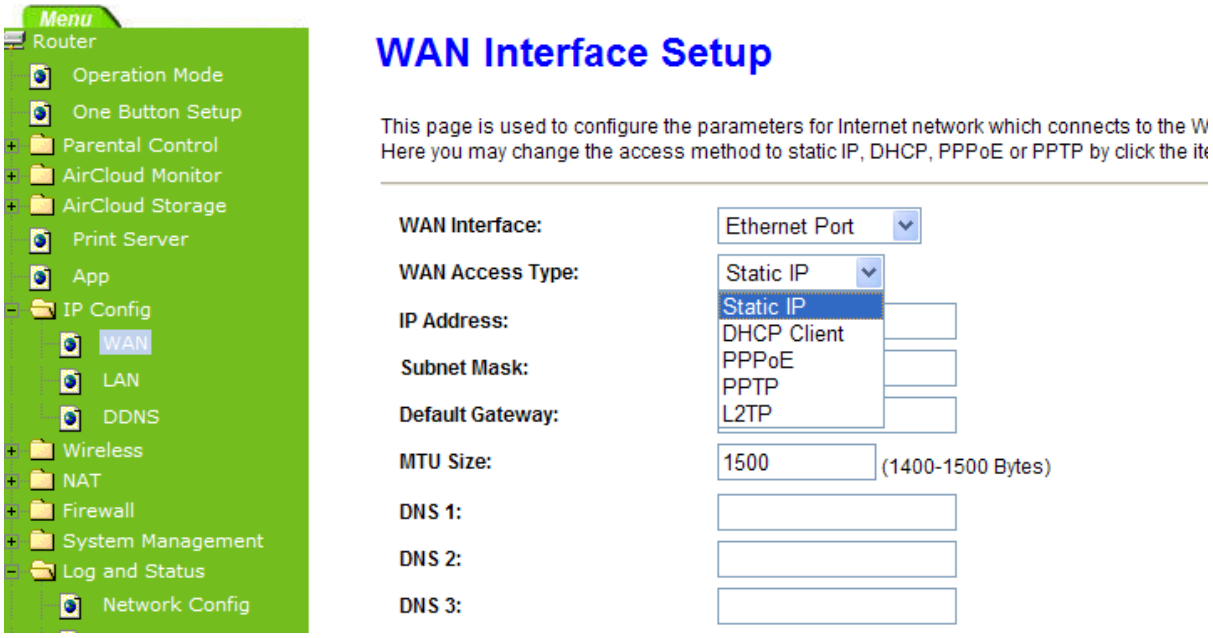
Enable FTP Access from WAN	Allow user access device FTP server from WAN side（internet）
FTP Server Port	Default FTP server port is 21
Idle Connection Time-Out	FTP process should have an idle timeout, which will terminate the process and close the control connection if the server is inactive (i.e., no command or data transfer in progress) for a long period of time

3.2.3.2 Samba management

Default is Share mode，user do not need account to access USB disk。If smaba application always need account for access USB dis，the samba security mode should be user mode（user mode login account is “admin”，do not need password）

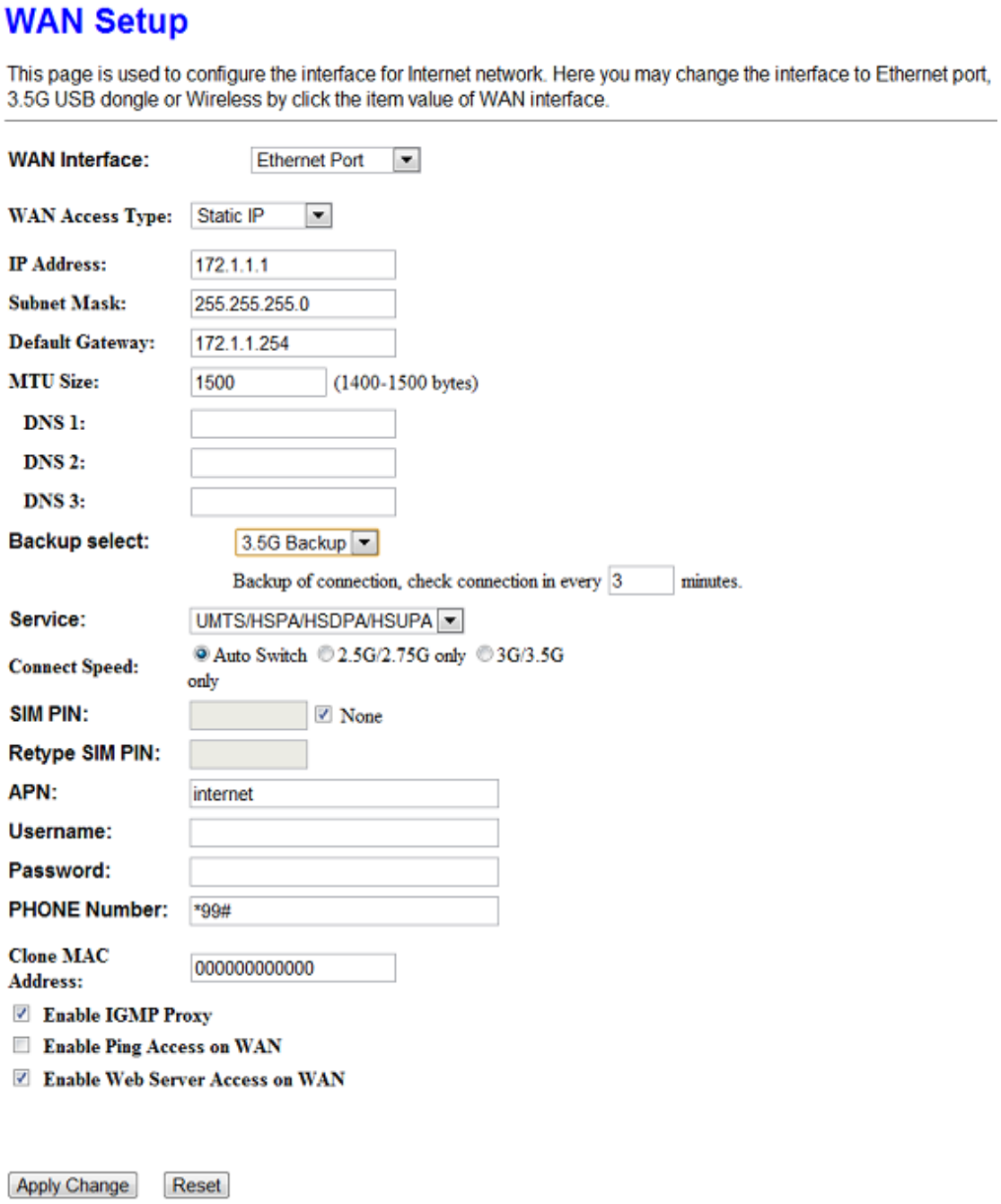
3.2.4 WAN Interface- Ethernet Port

The WAN access type is depended on the service that you contract with the provider. The GR-1736 provides five selections for the WAN access type, **Static IP, DHCP Client, PPPoE, PPTP and L2TP**. Check with your ISP if you don’t know the WAN type.



3.2.4.1 Static IP

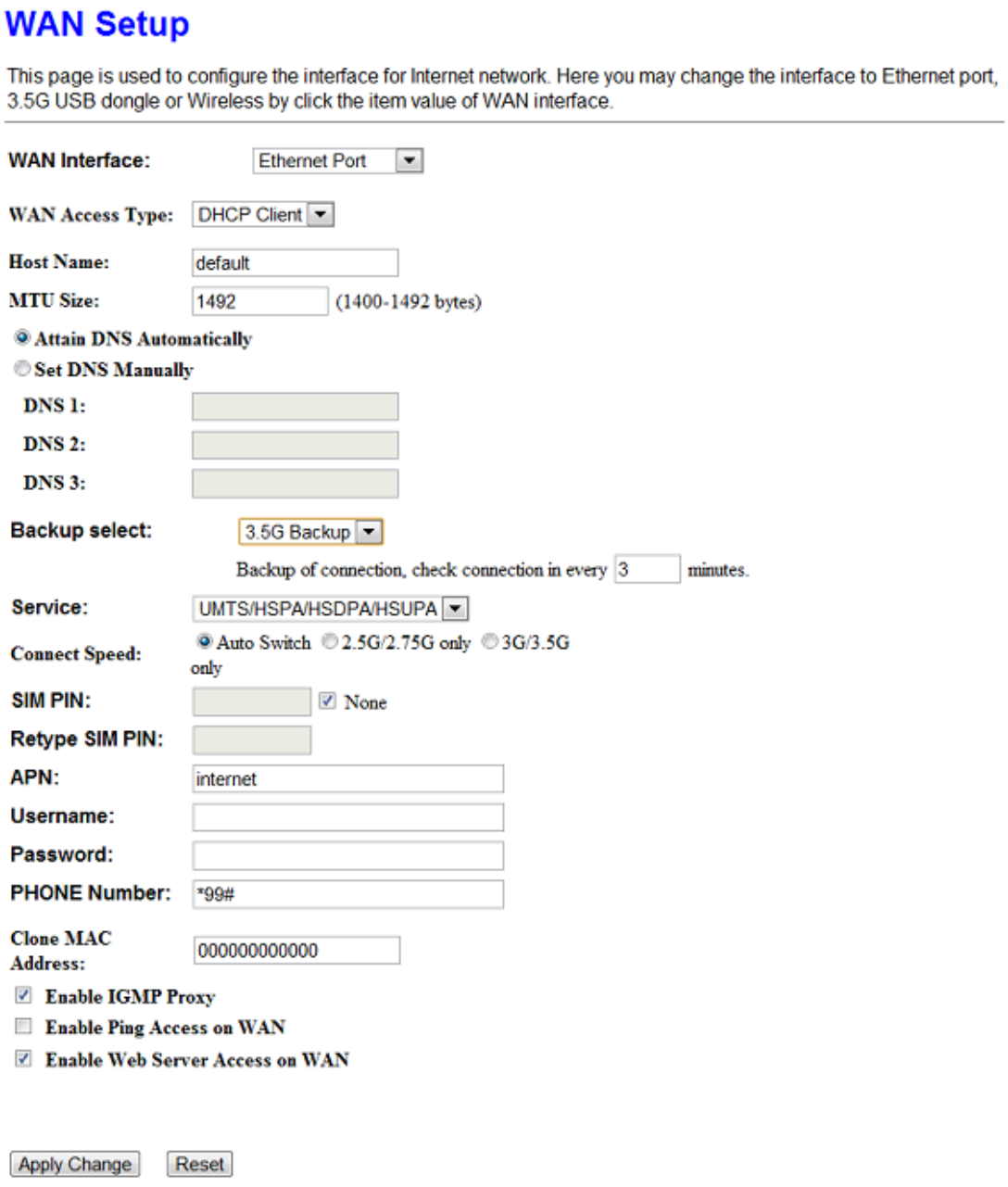
Select **WAN** under the **IP Config** menu, and choose Ethernet Port for the WAN Interface. Its associated setting will show up.


WAN Setup
This page is used to configure the interface for Internet network. Here you may change the interface to Ethernet port, 3.5G USB dongle or Wireless by click the item value of WAN interface.
WAN Interface: Ethernet Port
WAN Access Type: Static IP
IP Address: 172.1.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 172.1.1.254
MTU Size: 1500 (1400-1500 bytes)
DNS 1:
DNS 2:
DNS 3:
Backup select: 3.5G Backup
Backup of connection, check connection in every 3 minutes.
Service: UMTS/HSPA/HSDPA/HSUPA
Connect Speed: Auto Switch 2.5G/2.75G only 3G/3.5G only
SIM PIN: None
Retype SIM PIN:
APN: internet
Username:
Password:
PHONE Number: *99#
Clone MAC Address: 000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

Item	Description
WAN Access Type	Select **"Static IP"**
IP Address	Enter the IP address which is provided by your ISP.
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Input ISP Default Gateway Address, .
DNS	Input DNS information which is provided by your ISP
Backup select	Select 3G as a back up solution or none.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter

	the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

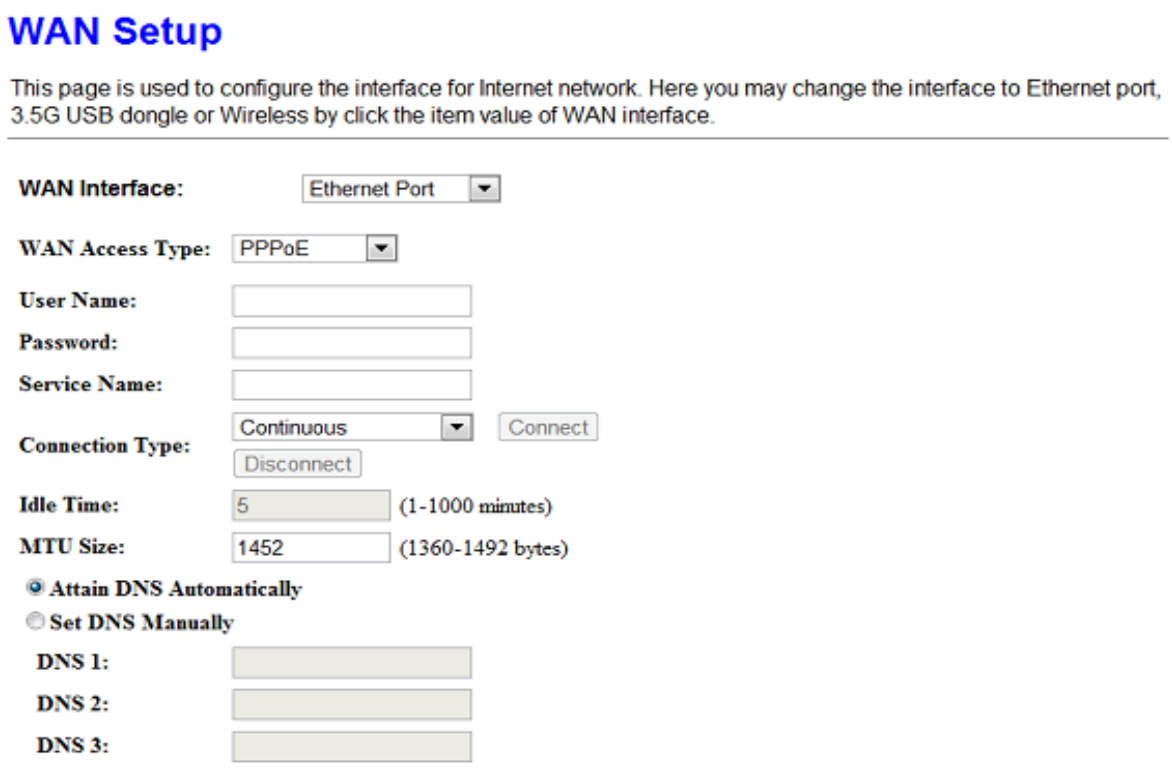
3.2.4.2 DHCP Client

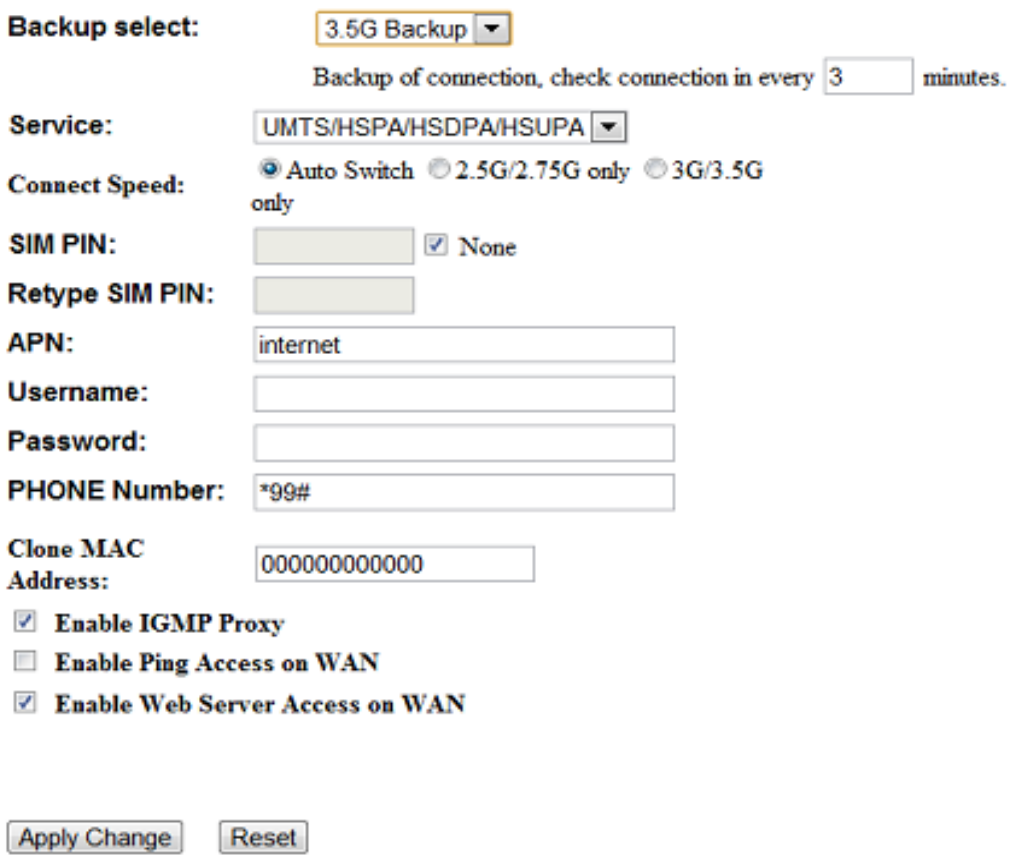


Item	Description
WAN Access Type	Select **"DHCP Client"**
Host Name	You can keep the default as the host name, or input a specific name if required by your ISP.

DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Backup select	Select 3G as a back up solution or none.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

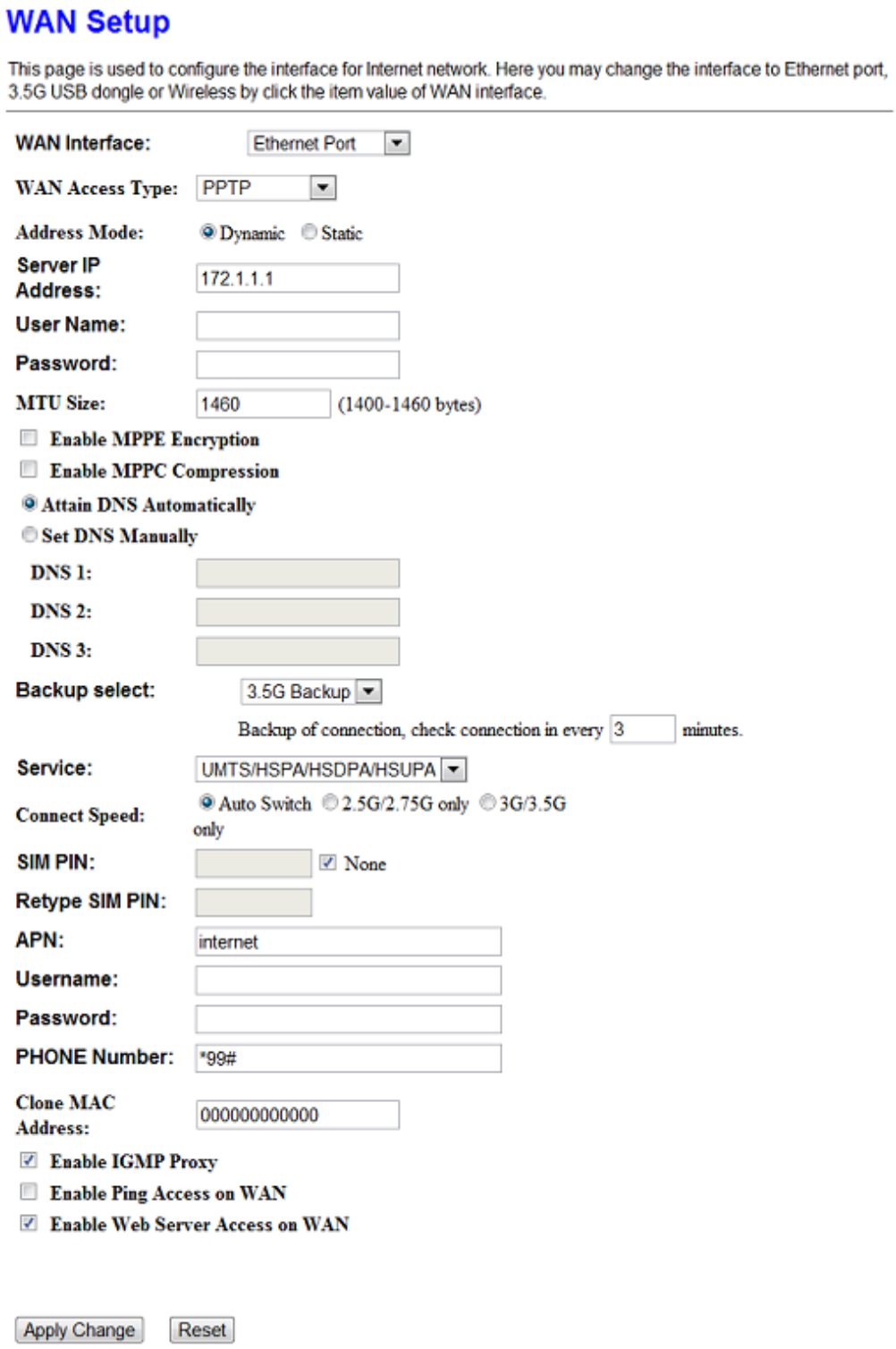
3.2.4.3 PPPoE





Item	Description
WAN Access Type	Select **"PPPoE"**
User Name	Input your user name provided by your ISP. If you don't know, please check with your ISP.
Password	Input the password provided by your ISP.
Service Name	Input the service name provided by your ISP.
Connection Type	Three types for select: **Continues, Connect on Demand,** and **Manual.**
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Backup select	Select 3G as a back up solution or none.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

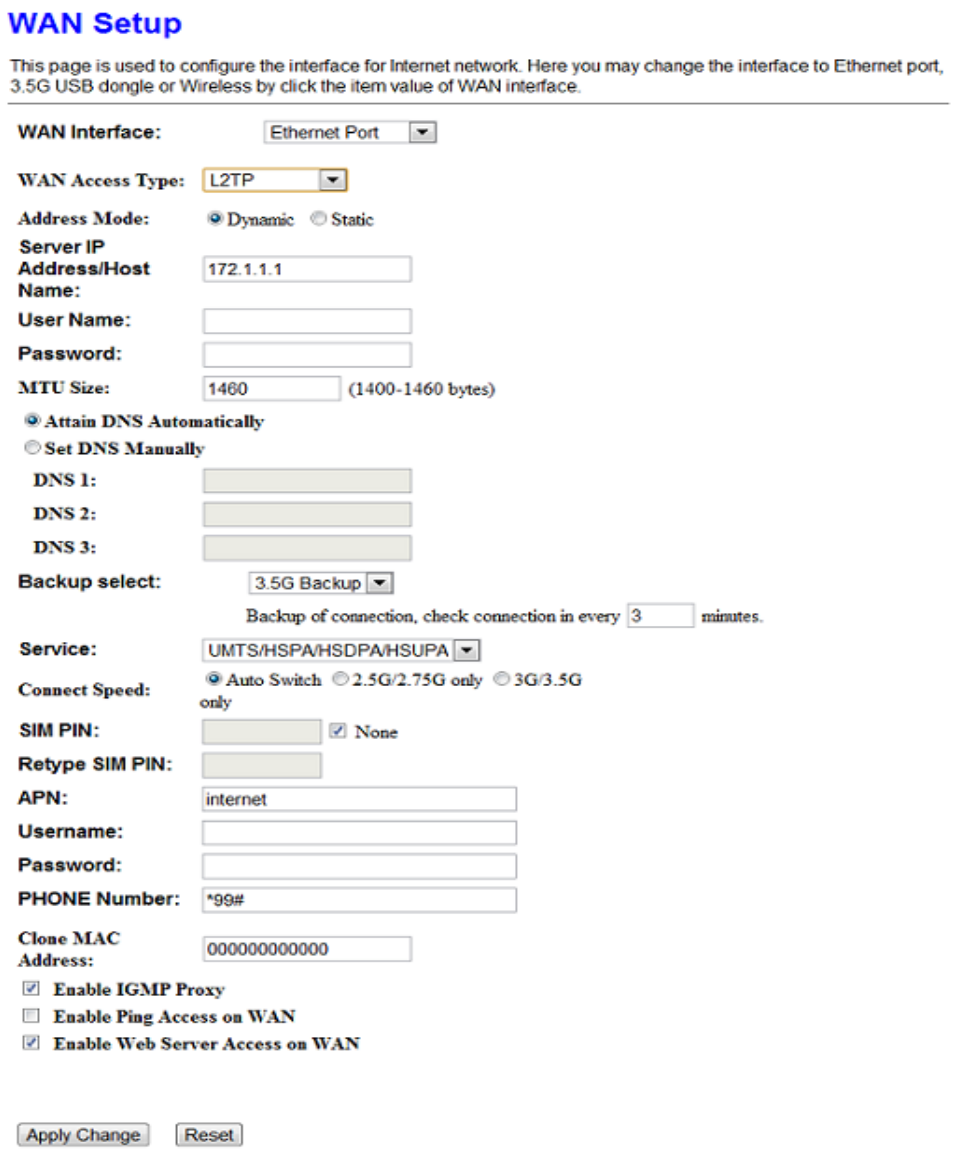
3.2.4.4 PPTP


WAN Setup
This page is used to configure the interface for Internet network. Here you may change the interface to Ethernet port, 3.5G USB dongle or Wireless by click the item value of WAN interface.
WAN Interface: Ethernet Port
WAN Access Type: PPTP
Address Mode: Dynamic Static
Server IP Address: 172.1.1.1
User Name:
Password:
MTU Size: 1460 (1400-1460 bytes)
Enable MPPE Encryption
Enable MPPC Compression
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Backup select: 3.5G Backup
Backup of connection, check connection in every 3 minutes.
Service: UMTS/HSPA/HSDPA/HSUPA
Connect Speed: Auto Switch 2.5G/2.75G only 3G/3.5G only
SIM PIN: None
Retype SIM PIN:
APN: internet
Username:
Password:
PHONE Number: *99#
Clone MAC Address: 000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

Item	Description
WAN Access Type	Select **"PPTP"**
Server IP Address	Input your server IP address provided by your ISP. If you don't know, please check with your ISP.

User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Backup select	Select 3G as a back up solution or none.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

3.2.4.5 L2TP


WAN Setup
This page is used to configure the interface for Internet network. Here you may change the interface to Ethernet port, 3.5G USB dongle or Wireless by click the item value of WAN interface.
WAN Interface: Ethernet Port
WAN Access Type: L2TP
Address Mode: Dynamic Static
Server IP Address/Host Name: 172.1.1.1
User Name:
Password:
MTU Size: 1460 (1400-1460 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Backup select: 3.5G Backup
Backup of connection, check connection in every 3 minutes.
Service: UMTS/HSPA/HSDPA/HSUPA
Connect Speed: Auto Switch 2.5G/2.75G only 3G/3.5G only
SIM PIN: None
Retype SIM PIN:
APN: internet
Username:
Password:
PHONE Number: *99#
Clone MAC Address: 000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

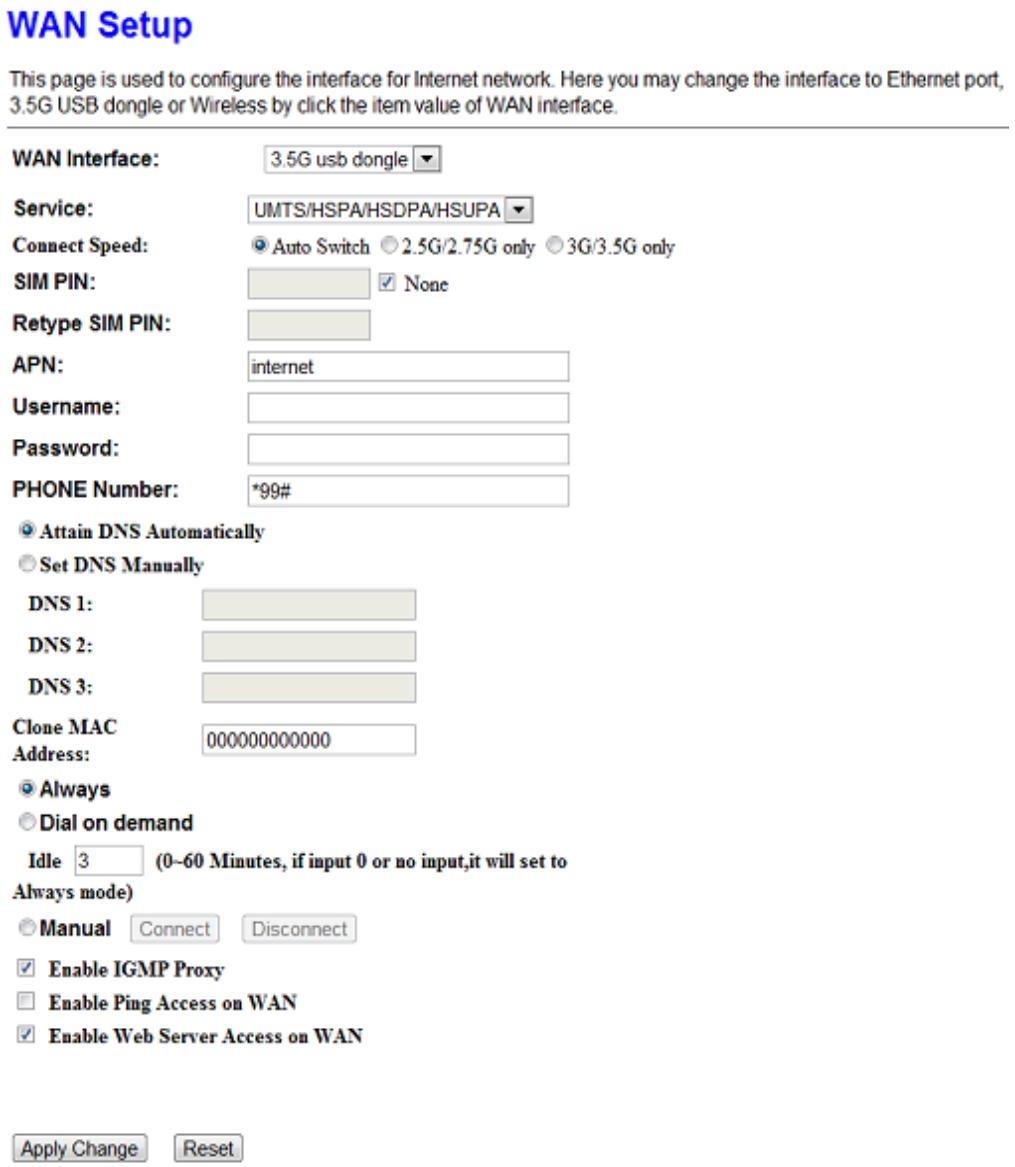
Item	Description
WAN Access Type	Select **"PPTP"**
Server IP Address / Host Name	Input your server IP address or Host Name provided by your ISP. If you don't know, please check with your ISP.
User Name	Input PPTP account provided by your ISP.
Password	Input the password provided by your ISP.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Backup select	Select 3G as a back up solution or none.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

3.2.4.6 Advance function

Item	Description
MTU	Maximum Transmission Unit. Usually provide by computer operation systems (OS). Advanced users can set it manually.
Request MPPE Encryption	Microsoft Point-to-Point Encryption (MPPE) provides data security for the PPTP connection that is between the VPN client and VPN server.
Enable IGMP Proxy	**Enable IGMP Proxy** to provide the service for IP hosts and adjacent multicast routers to establish multicast group memberships.
Enable Ping Access on WAN	**Enable Ping Access on WAN** will make WAN IP address response to any ping request from Internet users. However, it is also a comma way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.

3.2.5 WAN Interface- 3G USB dongle

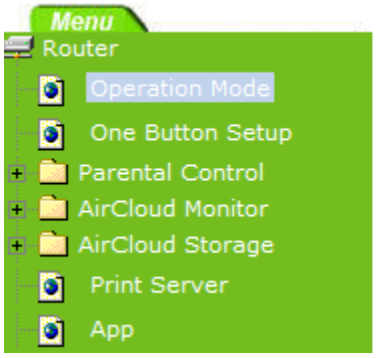
Select **WAN** under the **IP Config** menu, and choose 3G USB dongle for the WAN Interface. Its associated setting will show as below.



Item	Description
APN (Access Point Name)	Enter the access point name. If you do not know the setting information for APN, check with your 3G service provider.
User Name	Enter the User Name supplied by the provider.
Password	Enter the password supplied by the provider.
Phone Number	Enter the subscribing access point's phone number.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.

Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Always / Dial on demand	If your 3G USB adapter is a pay-as-you-go plan base, select “Dial on demand” and disconnect the connection when you don't use the internet.
Enable IGMP Proxy	**Enable IGMP Proxy** to provide the service for IP hosts and adjacent multicast routers to establish multicast group memberships.
Enable Ping Access on WAN	**Enable Ping Access on WAN** will make WAN IP address response to any ping request from Internet users. However, it is also a comma way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Change	Click **“Finish”** to complete the setting

Rebooting this product is started. Please wait for a while.

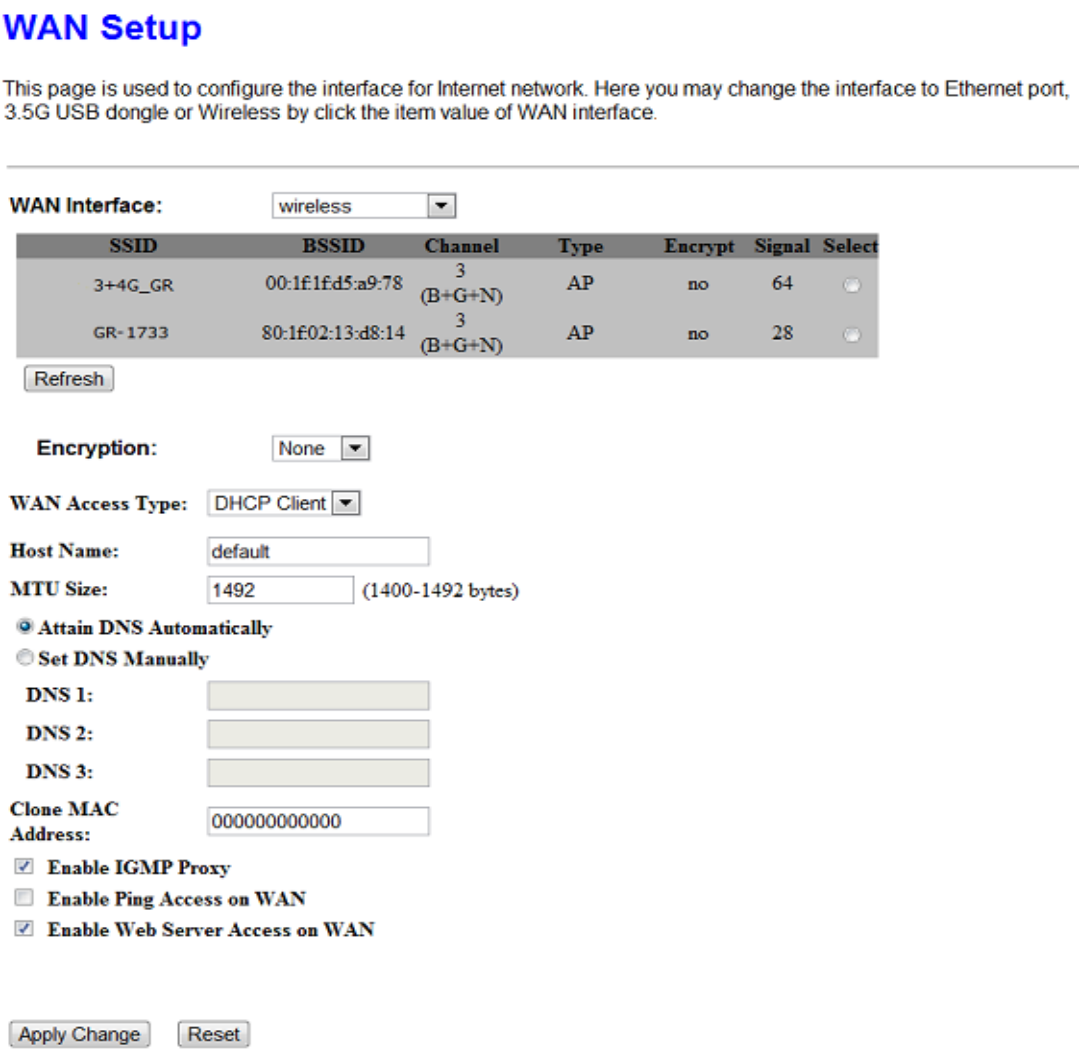


Change setting successfully!

System is configuring, after 19 seconds....

3.2.6 WAN Interface- Wireless

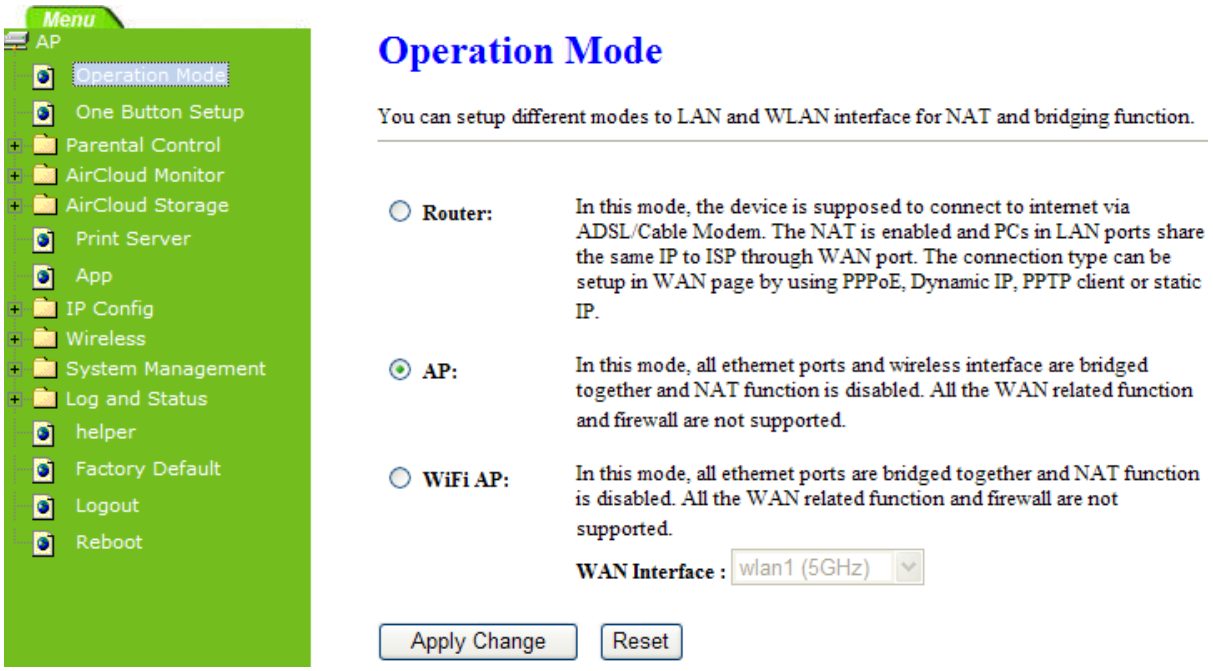
Select WAN under the IP Config menu, and choose wireless for the WAN Interface. Its associated setting will show as below.


WAN Setup
This page is used to configure the interface for Internet network. Here you may change the interface to Ethernet port, 3.5G USB dongle or Wireless by click the item value of WAN interface.
WAN Interface: wireless
SSID BSSID Channel Type Encrypt Signal Select
3+4G_GR 00:1f:1f:d5:a9:78 3 (B+G+N) AP no 64
GR-1733 80:1f:02:13:d8:14 3 (B+G+N) AP no 28
Refresh
Encryption: None
WAN Access Type: DHCP Client
Host Name: default
MTU Size: 1492 (1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address: 000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

Item	Description
Refresh	You can see a list of available Wireless networks. Select the preferred one.
Encryption type	Select the Encryption type form the drop-down list.
WAN Access Type	Select Static IP, DHCP, PPPoE, PPTP or L2TP.
DNS	Select **Attain DNS Automatically**. Or select **Set DNS Manually**, if you want to specify the DNS, and enter the DNS provided by your ISP in DNS 1 2 3.
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

3.3 AP Mode-Using as a Access Point

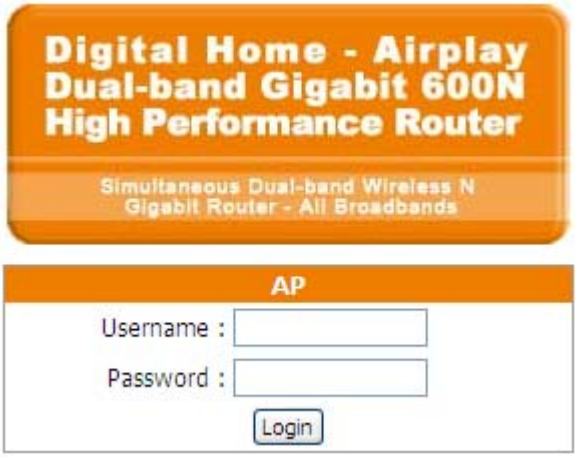
Make sure to shift the mode into AP Mode.


Menu
AP
Operation Mode
One Button Setup
Parental Control
AirCloud Monitor
AirCloud Storage
Print Server
App
IP Config
Wireless
System Management
Log and Status
helper
Factory Default
Logout
Reboot
Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, Dynamic IP, PPTP client or static IP.
AP:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
WiFi AP:
In this mode, all ethernet ports are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
WAN Interface :
wlan1 (5GHz)
Apply Change
Reset

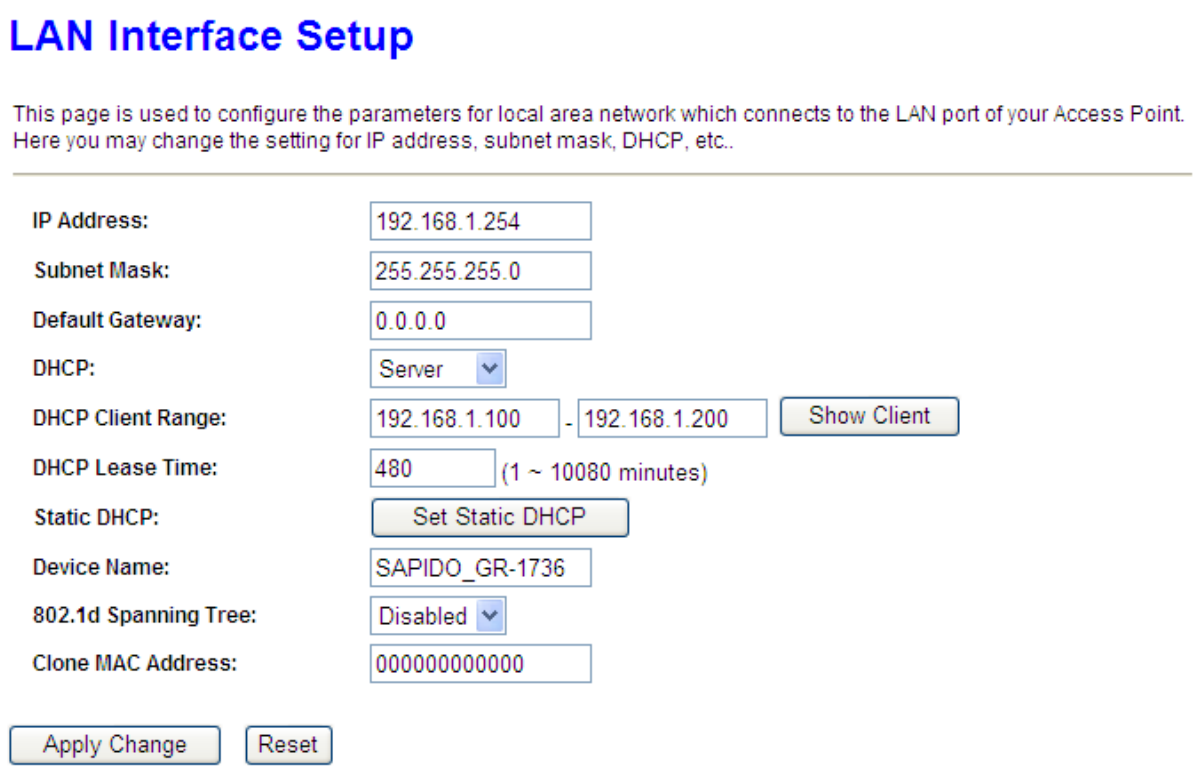
When this product is used as an access point, the IP address has to be changed. The default IP under AP mode is 192.168.1.254.

1. Open a Web browser, and enter http://192.168.1.254 (Default Gateway) into the blank.

2. Enter the User name and Password in to the blank and then Click **Login**. The default values for User Name and Password are **admin** (all in lowercase letters).



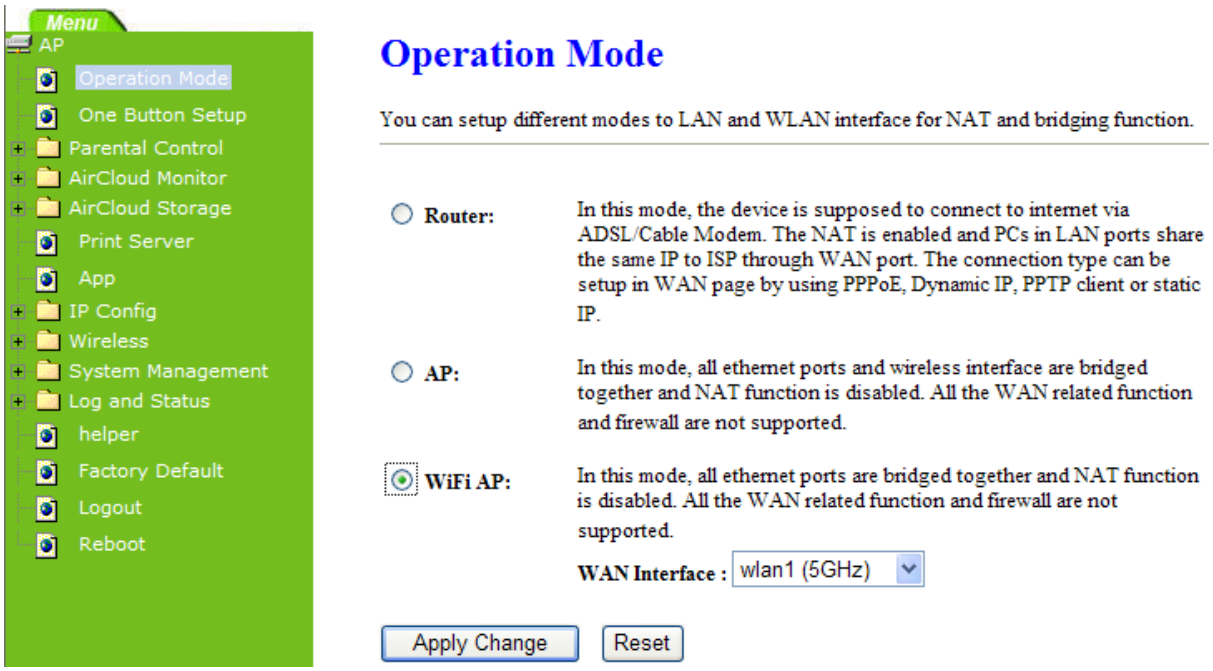
Select **LAN** under the **IP Config** menu



Item	Description
Device Name	Input a name for this router.
IP Address	The default IP address is 192.168.1.254
Subnet Mask	Enter the Subnet Mask address
Default Gateway	Enter the Default Gateway address for LAN interfaces
DHCP	Select DHCP type: **Client**, **Disable,** or **Server** under different environment.
DHCP Client Range	When enable DHCP server, you can fill in the start and end IP address; client will be assigned an IP address from the range.
802.1d Spanning Tree	Disable or Enable the 802.1d Spanning Tree Protocol (STP)
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

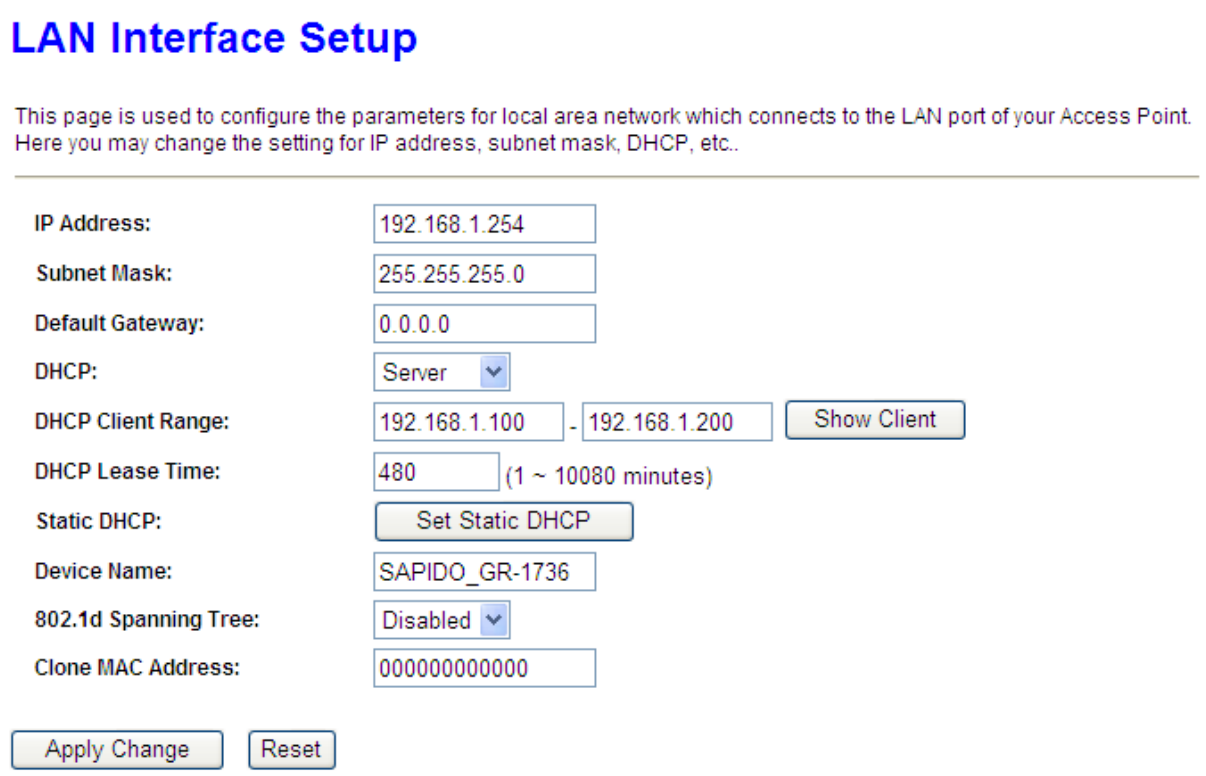
3.4 WiFi AP Mode- Using as a Network Converter

Make sure to shift the mode into WiFi AP Mode.


Menu
AP
Operation Mode
One Button Setup
Parental Control
AirCloud Monitor
AirCloud Storage
Print Server
App
IP Config
Wireless
System Management
Log and Status
helper
Factory Default
Logout
Reboot
Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, Dynamic IP, PPTP client or static IP.
AP:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
WiFi AP:
In this mode, all ethernet ports are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
WAN Interface :
wlan1 (5GHz)
Apply Change
Reset

The default gateway is http://192.168.1.254 and for User Name and Password are **admin** (all in lowercase letters). Click **Login** to enter.

Select **LAN** under the **IP Config** menu



Item	Description
Device Name	Input a name for this router.
IP Address	The default IP address is 192.168.1.254
Subnet Mask	Enter the Subnet Mask address
Default Gateway	Enter the Default Gateway address for LAN interfaces
DHCP	Select DHCP type: **Client**, **Disable,** or **Server** under different environment.
DHCP Client Range	When enable DHCP server, you can fill in the start and end IP address; client will be assigned an IP address from the range.
802.1d Spanning Tree	Disable or Enable the 802.1d Spanning Tree Protocol (STP)
Clone Mac Address	Some ISPs require MAC address registration. In this case, enter the MAC address registered to the provider to "Clone MAC Address"
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

Chapter 4 Wireless Setup

4.1 Wireless Setup

There are two ways to setup wireless LAN with GR-1736. You can use either way to setup Wireless LAN.

4.1.1 Setup Wireless LAN by WPS button

You can setup wireless LAN easily by using the WPS button if both WLAN router and the WLAN adapter (client) are WPS supported. Before starting the setup, please check the things below:

λ Get ready for Internet connection with GR-1736.

λ The WLAN adapter is finished installation and plug in your computer/ laptop.

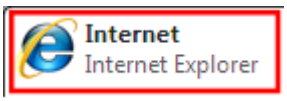
There are two ways to setup a wireless LAN between GR-1736 and your wireless adapter:

1. Setup with WPS button, if your wireless adapter has a physical WPS button.

(1) Press the WPS button from GR-1736 and wait for Wireless/WPS LED light changed into orange.

(2) Press the WPS button from the adapter until the setup window shows up.

(3) Open a web browser to check the internet connection.

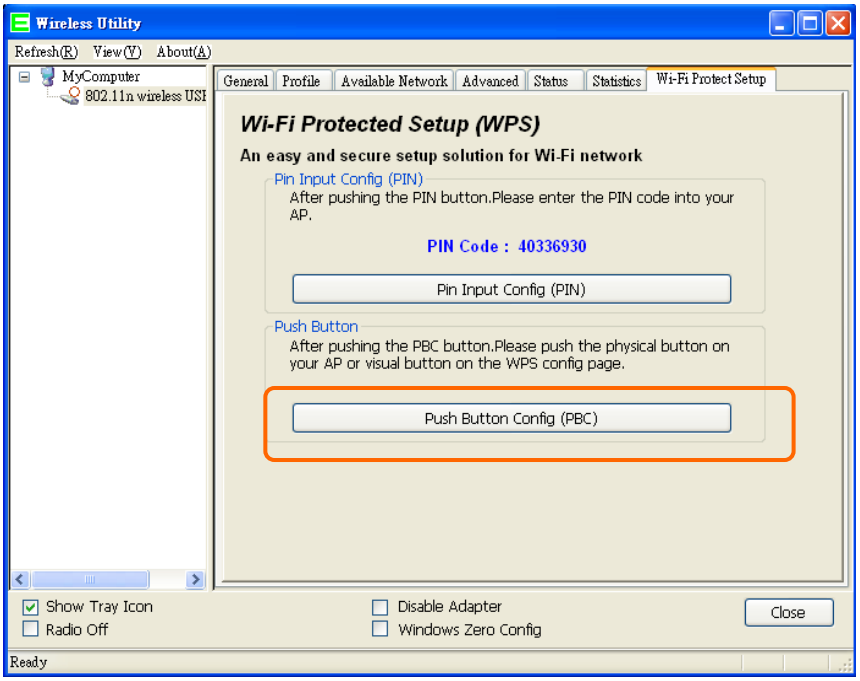


(4) Setup without WPS button if you wireless adapter has only virtual WPS function.

(5) Open Wireless adapter utility.

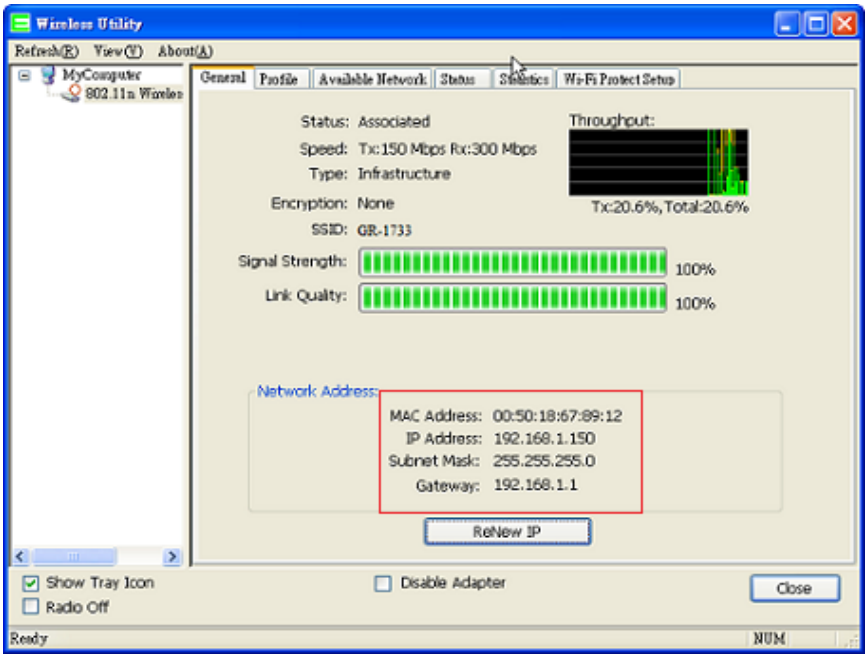
(6) Press the WPS button (A) from GR-1736 and wait for Wireless/WPS LED light (B) changed into orange.

(7) Back to the WLAN adapter utility and click its “PBC” (C) button.



The utility will start searching the destination connection.

(8) Confirm the information form the Utility

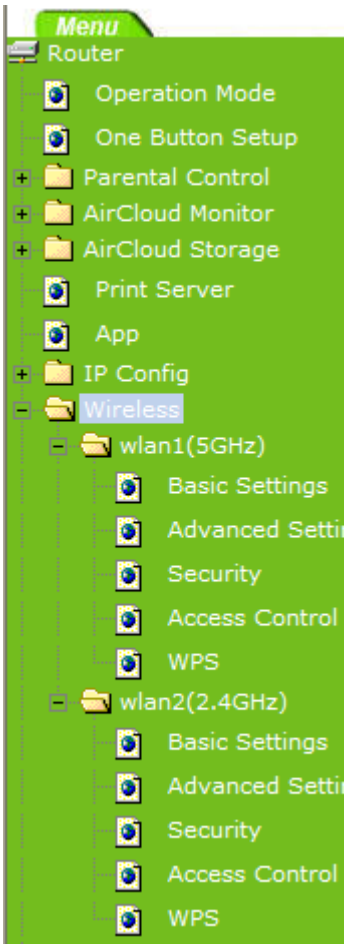


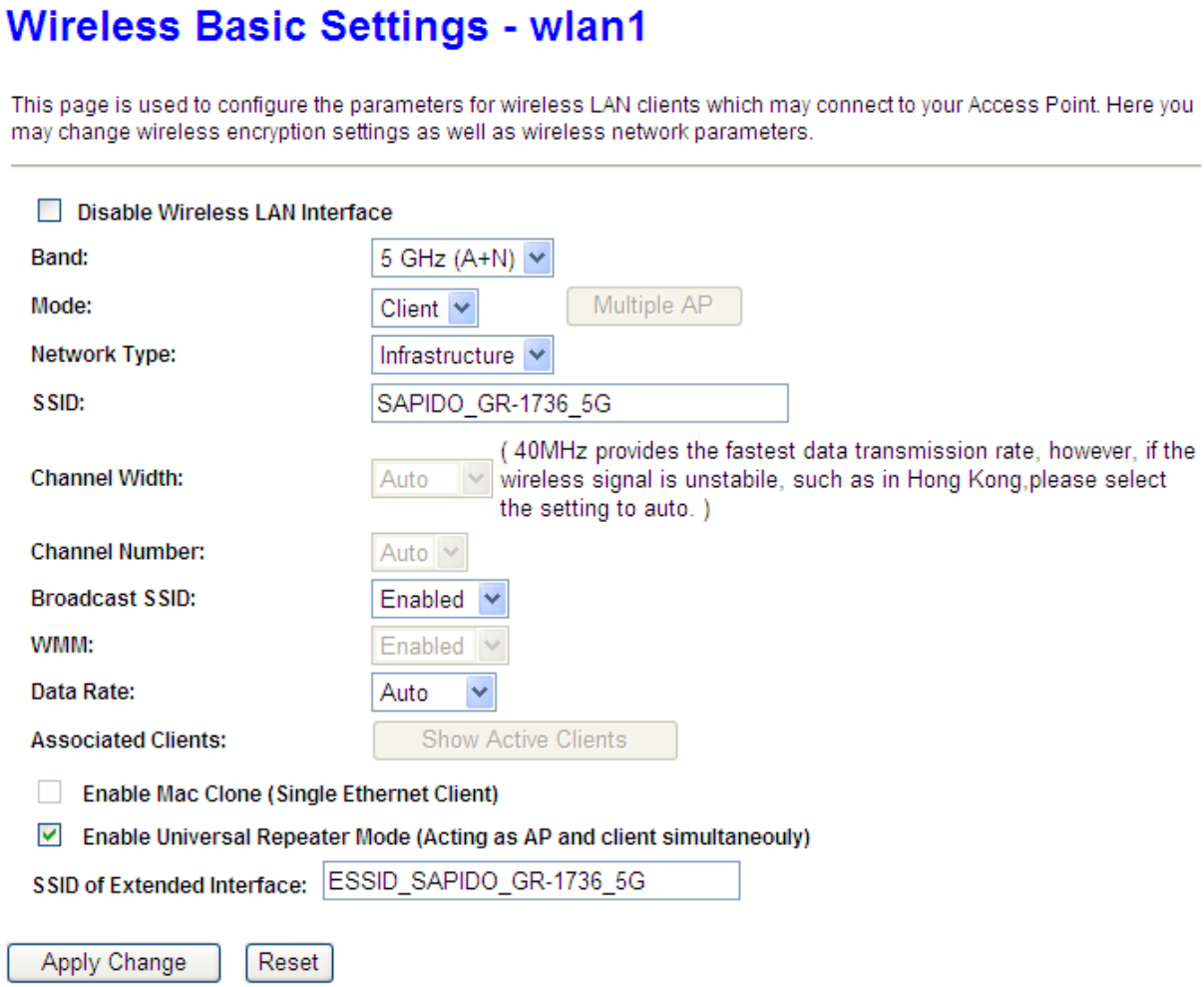
(9) After completes the WPS setup. Please confirm that it can be connected to the Internet.

Note: The setup image might be some differences when using other branded Adapter.

4.1.2 Wireless Basic Setup from Web GUI

The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.




Wireless Basic Settings - wlan1
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Disable Wireless LAN Interface
Band:
5 GHz (A+N)
Mode:
Client
Multiple AP
Network Type:
Infrastructure
SSID:
SAPIDO_GR-1736_5G
Channel Width:
Auto
(40MHz provides the fastest data transmission rate, however, if the wireless signal is unstabile, such as in Hong Kong,please select the setting to auto.)
Channel Number:
Auto
Broadcast SSID:
Enabled
WMM:
Enabled
Data Rate:
Auto
Associated Clients:
Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface:
ESSID_SAPIDO_GR-1736_5G
Apply Change
Reset

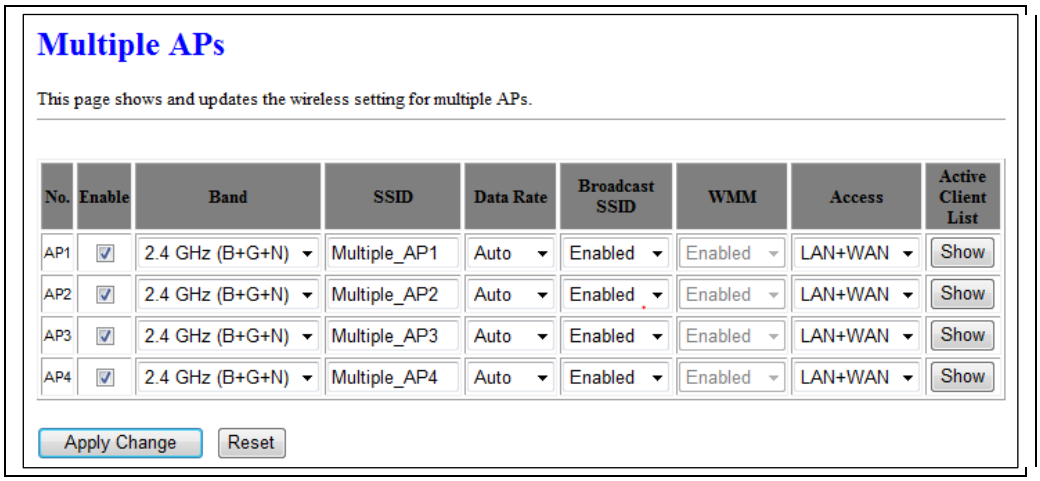
Item	Description
Disable Wireless LAN Interface	Turn off the wireless service.
2.4G Band	Select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
5G Band	Select the frequency. It has 3 options: 5 GHz (A / N / A+N).
Mode	Select the mode. It has 2 modes to select: (AP, Client,). Multiple AP * In Wi-Fi AP mode only support Client mode.
SSID	Service Set identifier, users can define to any or keep as default.
Channel Width	Please select the channel width, it has 3 options: Auto、20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.
2.4G Channel Number	Please select the channel; it has Auto, 1, 2~11 or 13 options.
5G Channel Number	Please select the channel; it has Auto, 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165.

Broadband SSID	User may choose to enable **Broadcast SSID** or not.
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Acting as AP and Client simultaneously)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.) Please also check Section 4.1.2.2
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

* Under WiFi AP Mode, there are 2 options of Network type: Infrastructure or Ad hoc. Select Infrastructure if connecting to a wireless router or access point. Select Ad hoc if connecting directly to another wireless adapter.

4.1.2.1 Multiple APs

The GR-1736 can support several SSIDs (wireless LAN group). It can be used as if there are multiple wireless LAN access points with one product. Each SSID could be set with different data rate, WMM and access type.



Item	Description
Enable	Enable or disable the service.
Band	Select the frequency.
SSID	Enter the SSID
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types:

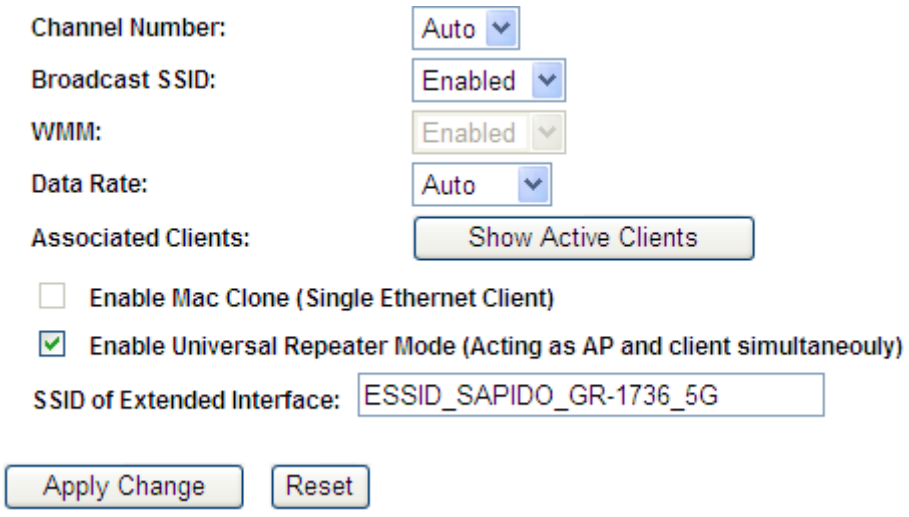
	a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.
Apply Change & Reset	Click on **Apply Change** to save the setting date, or you may click on **Reset** to clear all the input data.

4.1.2.2 Enable Universal Repeater Mode

The router can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

Example: When users enable the Universal Repeater to connect to the upper level device, please fill in the upper level devices channel and SSID. Click on Apply Changes to save the settings.

(Please disable the DHCP service first)


Channel Number: Auto
Broadcast SSID: Enabled
WMM: Enabled
Data Rate: Auto
Associated Clients: Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface: ESSID_SAPIDO_GR-1736_5G
Apply Change
Reset

Users can use the Network Configuration page to check the information about “Wireless Repeater Interface Configuration”.

4.2 Wireless Security Setup

Wireless 1 Configuration	
Mode	AP
Band	5 GHz (A+N)
SSID	11N_Broadband_Router_0d21ff
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
Wireless 2 Configuration	
Mode	AP
Band	2.4 GHz (N)
SSID	11N_Broadband_Router_0d21ff
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link.** There are five Encryption types supported: “None”, “WEP”, “WPA (TKIP)”, ”WPA2(AES)”, and “WPA2 Mixed”. Enabling WEP can protect your data from eavesdroppers. If you do not need this feature, select “None” to skip the following setting.

1. Encryption- WEP Key

(1) Set WEP Key: This section provides 64bit and 128bit WEP encryptions and two different shared key formats (ASCII and Hex) for wireless network.

(2) 802.1x Authentication

It is a safety system by using authentication to protect your wireless network.

2. Encryption- WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode

(1) Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password

(2) Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters.

(3) Apply Change & Reset: Click on 'Apply Changes' to save setting data. Or click 'Reset' to reset all the input data.

4.3 Wireless Access Control

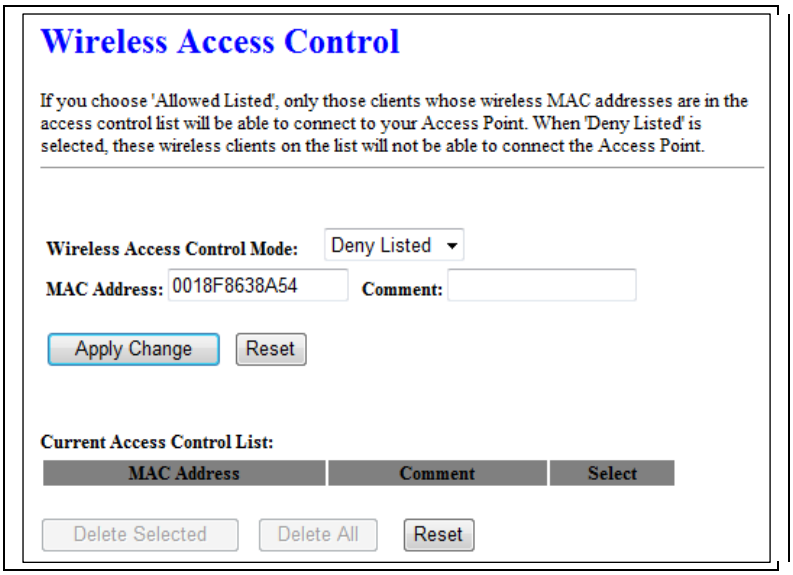
Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on "Apply Change" to save the new addition. To delete a MAC address, select its corresponding checkbox under the Select column and click on "Delete Selected" button.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Disable
MAC Address:
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Take the wireless card as the example.

(1) Please select Deny Listed in Wireless Access Control Mode first, and then fill in the MAC

address what you plan to block in the MAC Address field. Click Apply Changes to save the setting.


Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
0018F8638A54
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

(2) The MAC address what you set will be displayed on the Current Access Control List.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
00:18:f8:63:8a:54
Delete Selected
Delete All
Reset

(3) The wireless client will be denied by the wireless router.

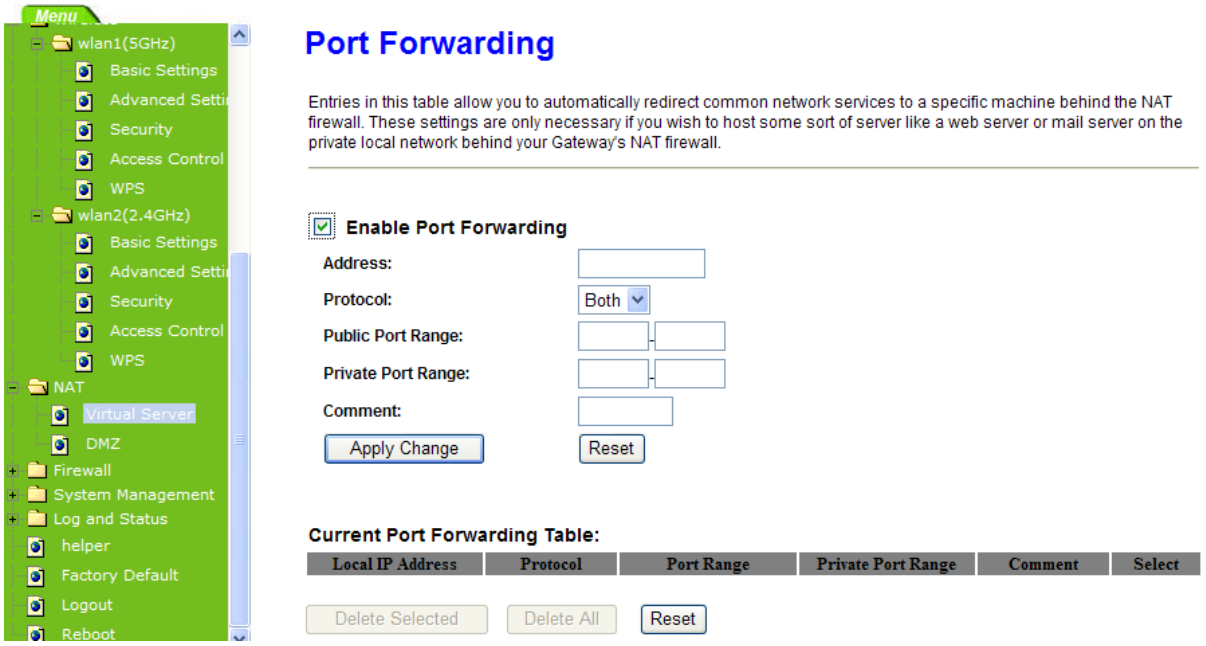
Chapter 5 Router Mode Security Setup

This section contains configurations for the GR-1736's advanced functions such as: virtual server, DMZ, and Firewall to provide your network under a security environment.

5.1 NAT

5.1.1 Virtual Server

The Virtual Server feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.

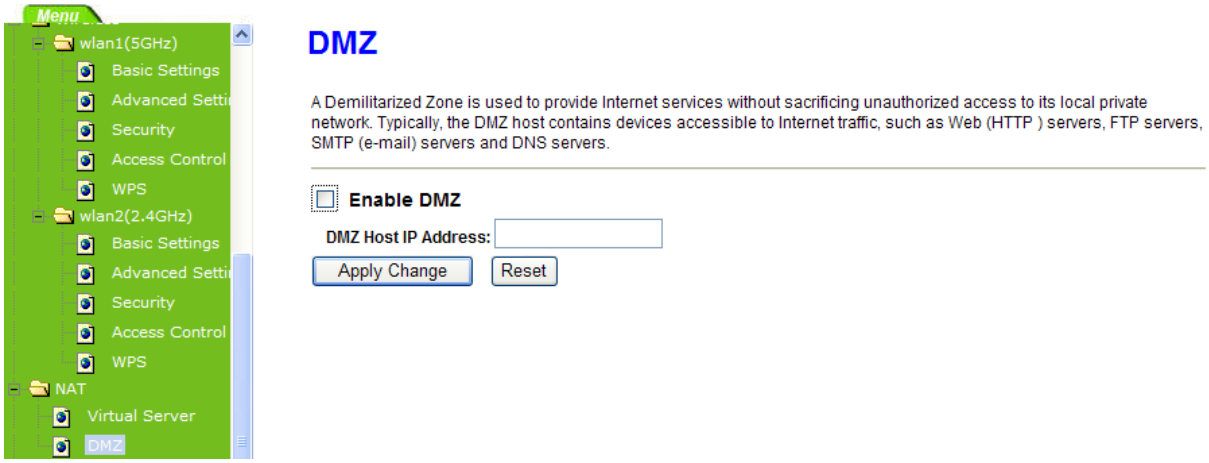


Item	Description
Enable Port Forwarding	Select to enable Port Forwarding service or not.
IP Address	Specify the IP address which receives the incoming packets.
Protocol	Select the protocol type.
Public Port Range	Enter the port number, for example 80-80.
Private Port Range	Enter the port number, for example 20-22.
Comment	Add comments for this port forwarding rule.
Add	Click on **Add** to enable the settings.
Current Port Forwarding Table	It will display all port forwarding regulation you made.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	Click **Reset** to cancel.

Please find the following figure to know that what the virtual server is. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.

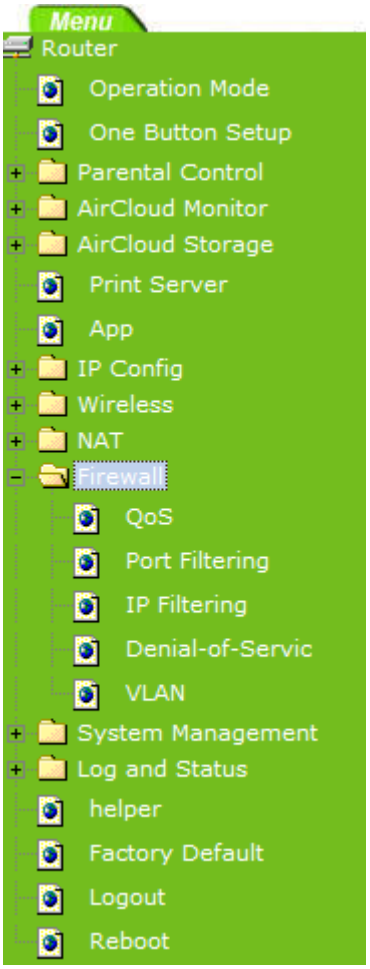
5.1.2 DMZ

The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application.



Item	Description
Enable DMZ	It will enable the DMZ service if you select it.
DMZ Host IP Address	Please enter the specific IP address for DMZ host.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

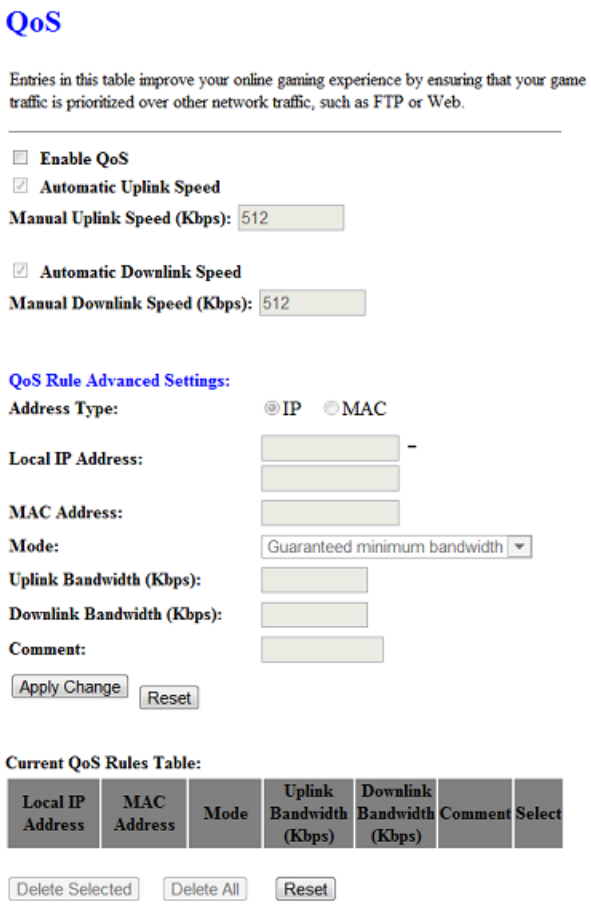
5.2 Firewall


Menu
Router
Operation Mode
One Button Setup
Parental Control
AirCloud Monitor
AirCloud Storage
Print Server
App
IP Config
Wireless
NAT
Firewall
QoS
Port Filtering
IP Filtering
Denial-of-Servic
VLAN
System Management
Log and Status
helper
Factory Default
Logout
Reboot

5.2.1 QoS

The QoS can let you classify Internet application traffic by source/destination IP address and port number.

To assign priority for each type of application and reserve bandwidth can let you have a better experience in using critical real time services like Internet phone, video conference …etc.

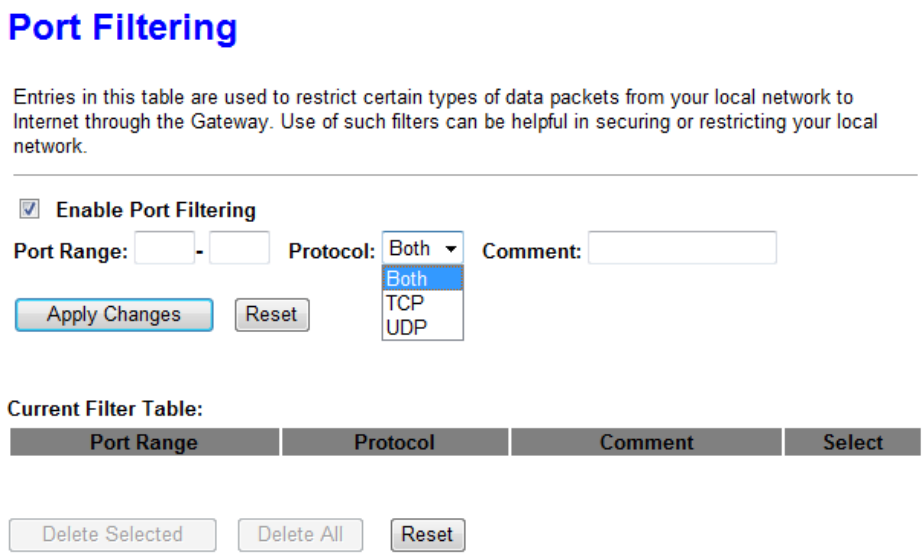


Item	Description
Enable QoS	Check “Enable QoS” to enable QoS function for the WAN port. You also can uncheck “Enable QoS” to disable QoS function for the WAN port.
Automatic uplink speed / Manual Uplink Speed	Set the uplink speed by manual to assign the download or upload bandwidth by the unit of Kbps or check the Automatic uplink speed.
Automatic downlink speed / Manual Downlink Speed	Set the downlink speed by manual to assign the download or upload bandwidth by the unit of Kbps or check the Automatic downlink speed.

QoS Rule Advance Setting:	
Address Type	Set QoS by **IP** Address or **MAC** address
Local IP Address	Set local IP Address if the address type is by IP Address
MAC Address	Set MAC Address if the address type is by MAC Address
Mode	Select **Guaranteed minimum bandwidth** or **Restricted maximum bandwidth**
Bandwidth	Key in the bandwidth.
Comment	Write your comment here.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2.2 Port Filtering

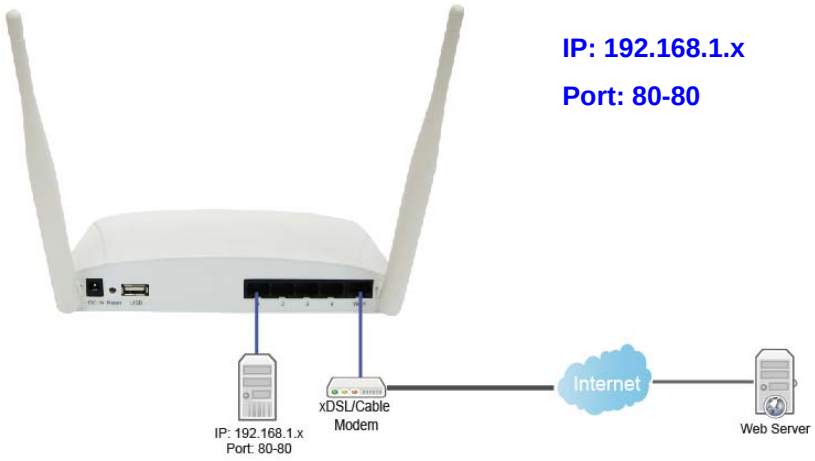
When enabled packets are denied access to Internet/filtered based on their port address.



Item	Description
Enable Port Filtering	Select Enable Port Filtering to filter ports.
Port Range	Enter the port number that needs to be filtered.
Protocol	Please select the protocol type of the port.
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete	Click **Delete Selected** will delete the selected item. Click **Delete All**

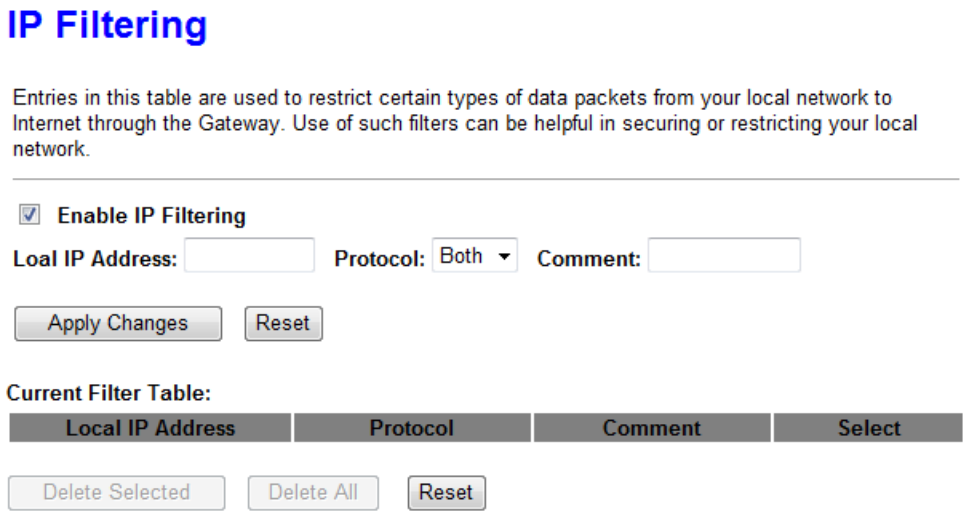
All	will delete all items in this table.
Reset	You can click **Reset** to cancel.

Port 80 has been blocked as the following illustrate.



5.2.3 IP Filtering

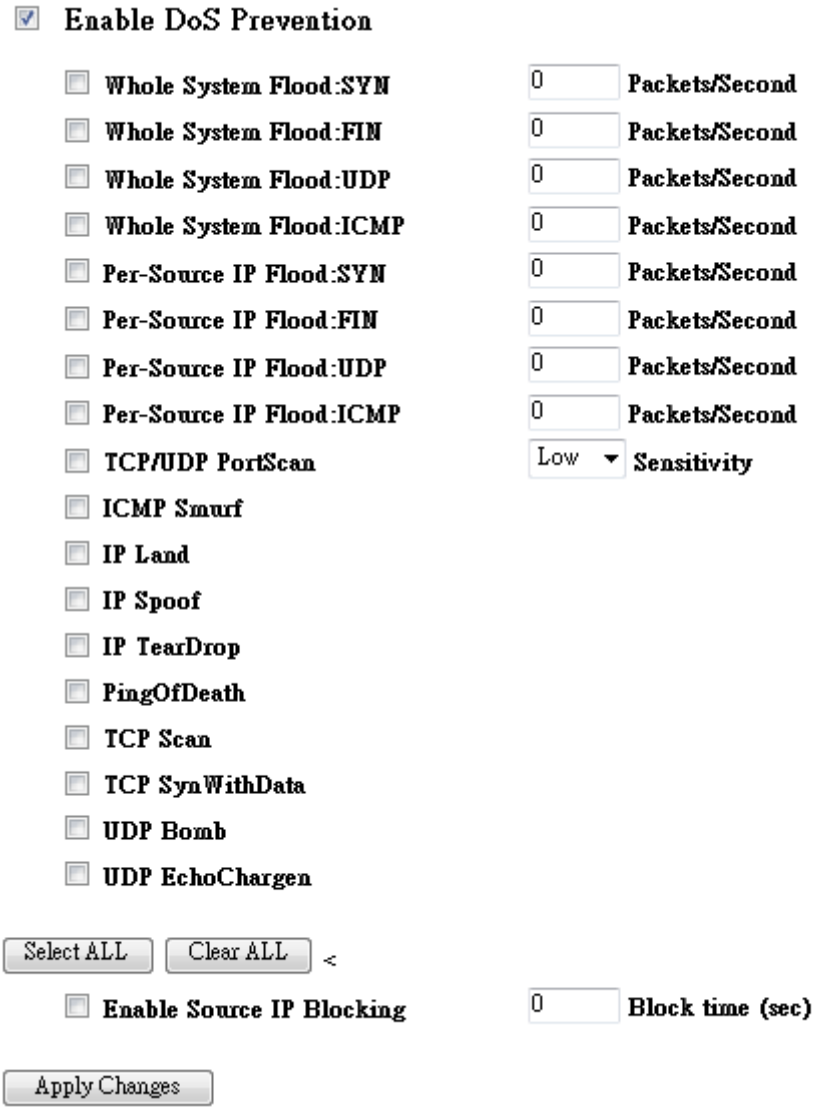
When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses.



Item	Description
Enable IP Filtering	Please select Enable IP Filtering to filter IP addresses.
Local IP Address	Please enter the IP address that needs to be filtered.

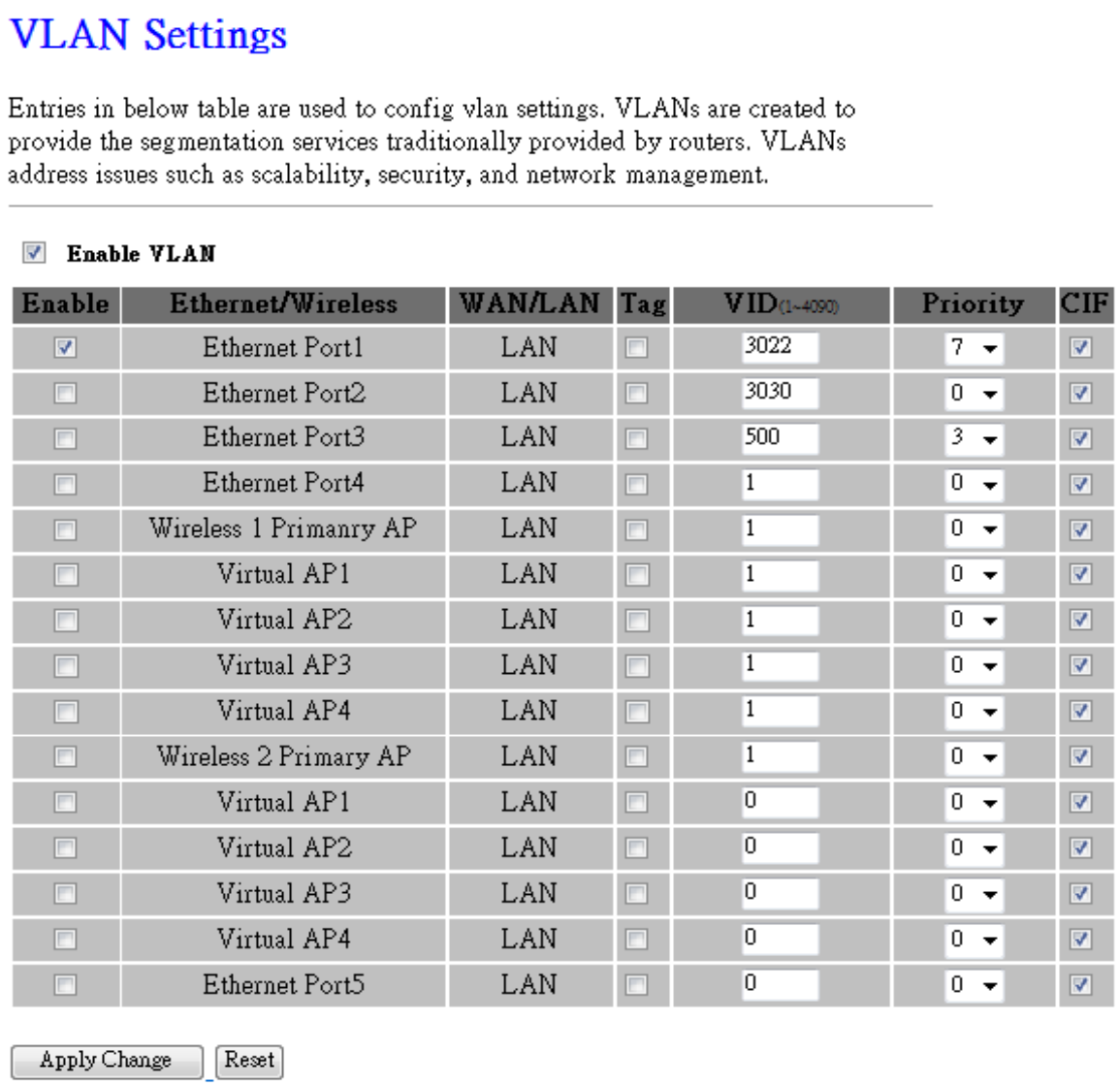
Protocol	Please select the protocol type of the IP address
Comment	You can add comments for this regulation.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	You can click **Reset** to cancel.

5.2.4 Denial of Service



Item	Description
Enable DoS Prevention	Check “Enable DoS Prevention” to enable DoS function for prevention. You also can uncheck ““Enable DoS Prevention” to disable DoS function.

5.2.5 VLAN Settings


VLAN Settings
Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.
Enable VLAN
Enable
Ethernet/Wireless
WAN/LAN
Tag
VID(1~4090)
Priority
CIF
Ethernet Port1 LAN 3022 7
Ethernet Port2 LAN 3030 0
Ethernet Port3 LAN 500 3
Ethernet Port4 LAN 1 0
Wireless 1 Primanry AP LAN 1 0
Virtual AP1 LAN 1 0
Virtual AP2 LAN 1 0
Virtual AP3 LAN 1 0
Virtual AP4 LAN 1 0
Wireless 2 Primary AP LAN 1 0
Virtual AP1 LAN 0 0
Virtual AP2 LAN 0 0
Virtual AP3 LAN 0 0
Virtual AP4 LAN 0 0
Ethernet Port5 LAN 0 0
Apply Change
Reset

Item	Description
Tag	Add VLAN tag to packet
VID	Set VLAN ID（1~4096）
Priority	It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority
CIF	Enable or Disable CIF

5.3 Server Setup

5.3.1 Webcam server

1. **USB port information**
   Show Link webcam information
2. **Enabling webcam**
   Enable or disable the webcam
3. **Control from the WAN side**
   Whether to allow viewing webcam images from the WAN
4. **Port webcam**
5. **Connection port view webcam**
6. **View live webcam video watch**
7. **Record Setup**

Save form:
Provide two formats AVI and JPG

Save location

If the captured image saved to a remote FTP location, be into a remote FTP location

maximum Recording Frames：

How many frames in one folder

Note：a JPG file size is about 13KB, and AVI file size is about 45127KB (when maximum recording frames is 1000), file size may vary due to webcam models have different sizes

Chapter 6 Advanced Setup

You can find advanced settings in this section.

Router Router Mode only.

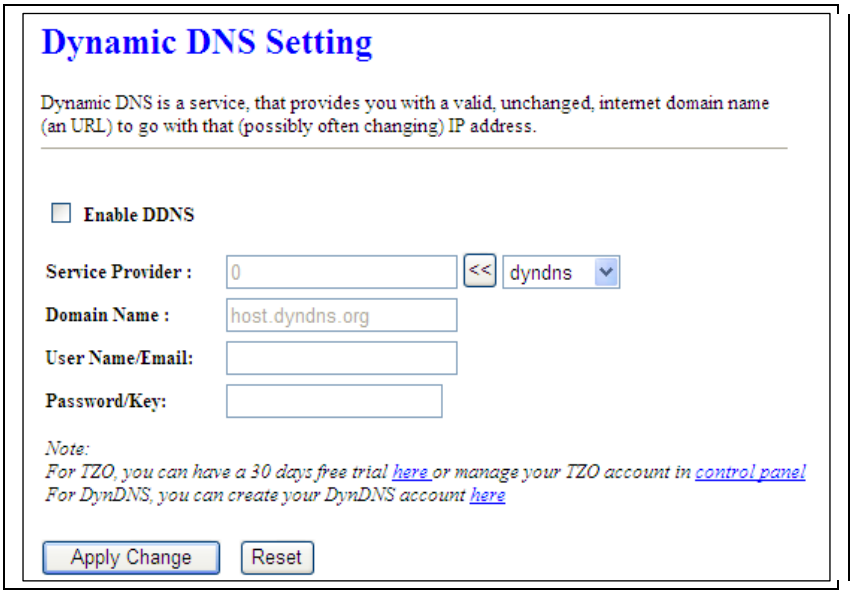
AP AP Mode only.

WiFi-AP WiFi AP Mode only.

6.1 Dynamic DNS Setting Router

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

Note: make sure that you have registered with a DDNS service provider before enabling this feature.

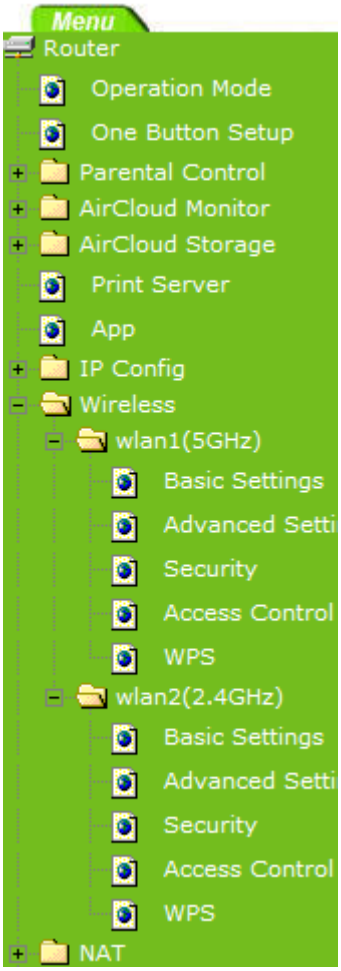

Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanged, internet domain name (an URL) to go with that (possibly often changing) IP address.
Enable DDNS
Service Provider :
0
<<
dyndns
Domain Name :
host.dyndns.org
User Name/Email:
Password/Key:
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Change
Reset

Please enter Domain Name, User Name/Email, and Password/Key. After entering, click on Apply Changes to save the setting, or you may click on Reset to clear all the input data.

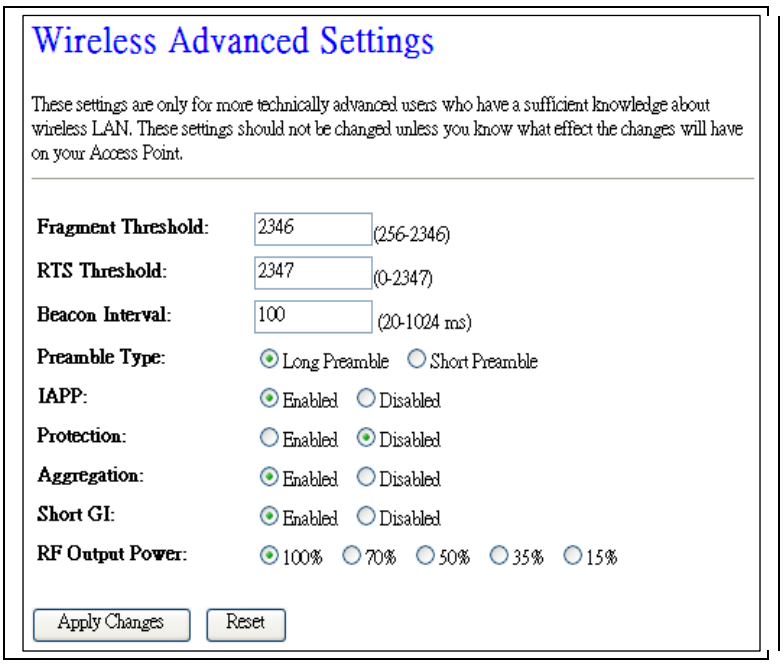
Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish embedded in GR-1736.

User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2 Wireless Advanced Setup



In Advanced Settings page, more 802.11 related parameters are tunable.


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Changes
Reset

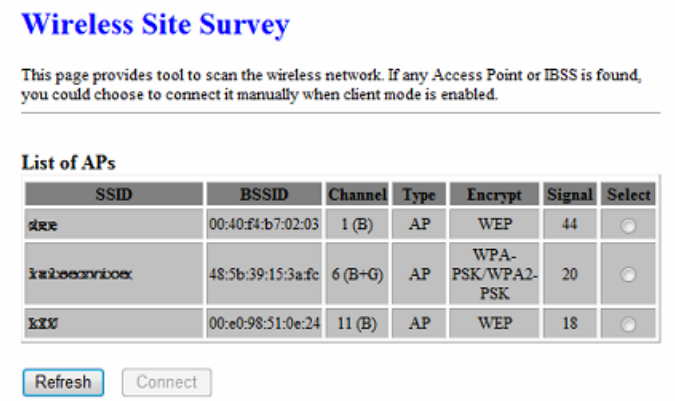
Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms..
Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and

	15%.
Apply Changes & Reset	Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.2.1 Wireless Site Survey WiFi-AP

This function provides users to search existing wireless APs or wireless base stations from ISP. You can connect to a wireless AP manually in Wi-Fi AP mode. The designed AP will appear on SSID column in Wireless Basic Setup page.

Please click on Refresh to refresh the list. Click Connect after select an existing AP to connect.



6.2.2 WPS Router AP

This page allows user to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize it's setting and connect to the Access Point in a minute without any hassle. GR-1736 could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

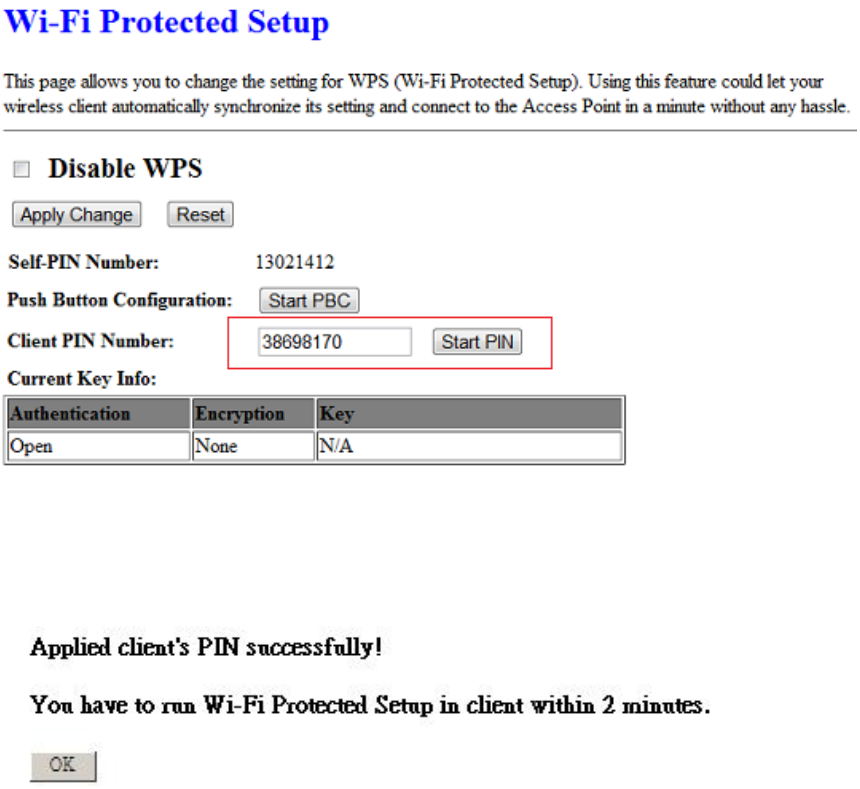
Please follow instructions below to enable the WPS function.

1. Setup Wireless LAN with WPS PIN :

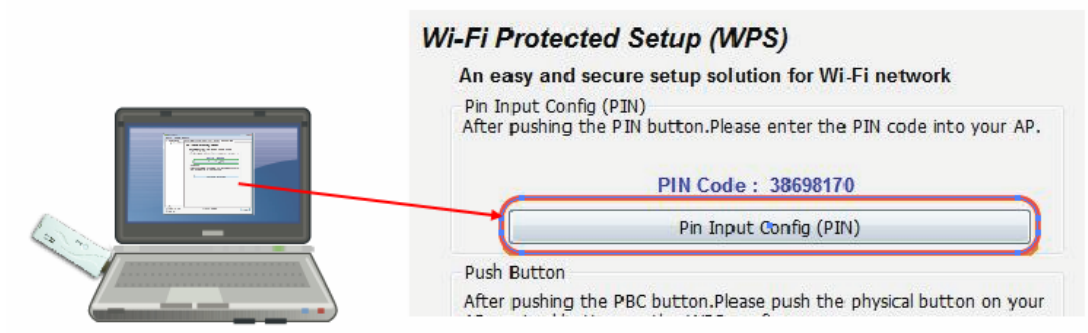
(1). Get the WPS PIN number from wireless card and write it down.

Wi-Fi Protected Setup (WPS)
An easy and secure setup solution for Wi-Fi network
Pin Input Config (PIN)
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 38698170
Pin Input Config (PIN)
Push Button
After pushing the PBC button.Please push the physical button on your

(2). Fill in the PIN number from the wireless card in Client PIN Number field, and then click “Start PIN”.


Wi-Fi Protected Setup
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.
Disable WPS
Apply Change
Reset
Self-PIN Number: 13021412
Push Button Configuration: Start PBC
Client PIN Number: 38698170 Start PIN
Current Key Info:
Authentication Encryption Key
Open None N/A
Applied client's PIN successfully!
You have to run Wi-Fi Protected Setup in client within 2 minutes.
OK

(3). Click PIN from Adapter Utility to complete the WPS process with the wireless router.

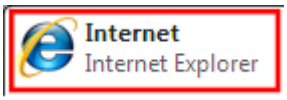

Wi-Fi Protected Setup (WPS)
An easy and secure setup solution for Wi-Fi network
Pin Input Config (PIN)
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 38698170
Pin Input Config (PIN)
Push Button
After pushing the PBC button.Please push the physical button on your

2. Start PBC:

(1). Press the WPS button (A) from GR-1736 and wait for Wireless/WPS LED light (B) changed into orange.

(2). Press the WPS button (C) from the adapter until the setup window shows up.

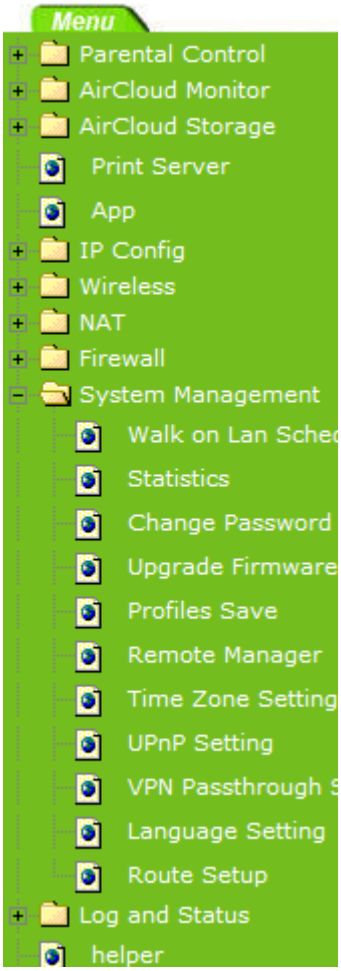
(3). Open a web browser to check the internet connection.



Please also refer to section 4.1.1 WPS setup for more details.

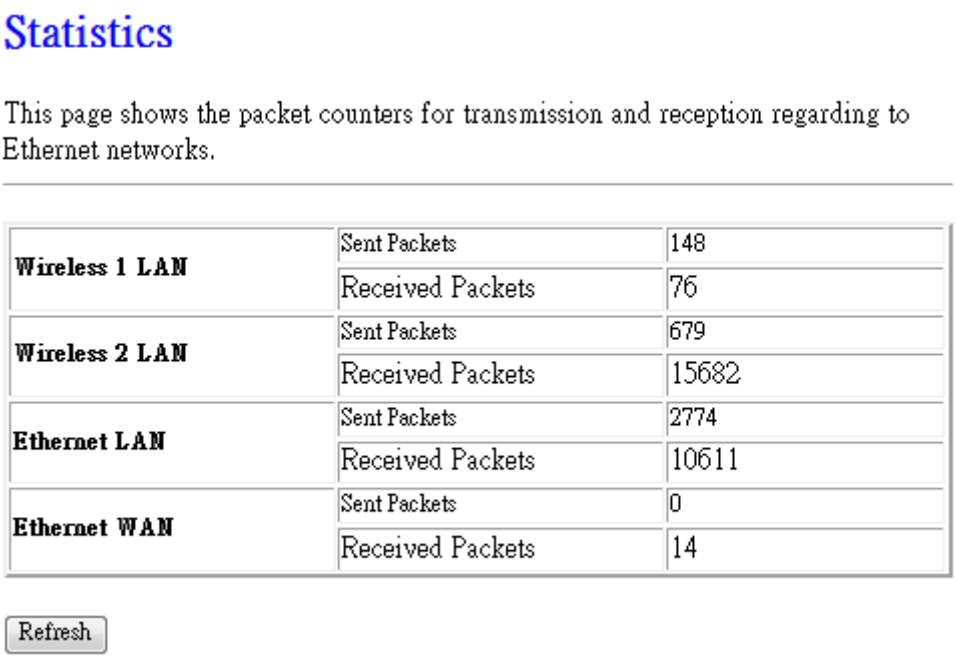
6.3 System Management

This section including **Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, VPN Passthrough Setting, and Language Setting**. It is easy and helpful for users making more detailed settings.



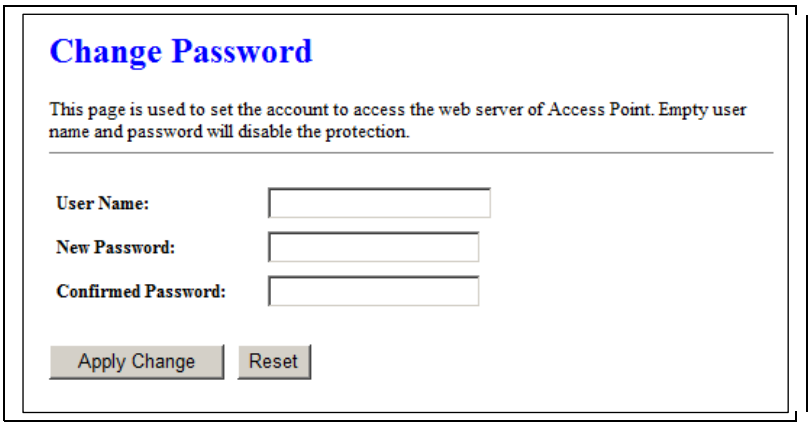
6.3.1 Statistics

It shows the packet counters for transmission and reception regarding to Ethernet networks



6.3.2 Change Password

Users can set or change user name and password used for accessing the web management interface in this section.

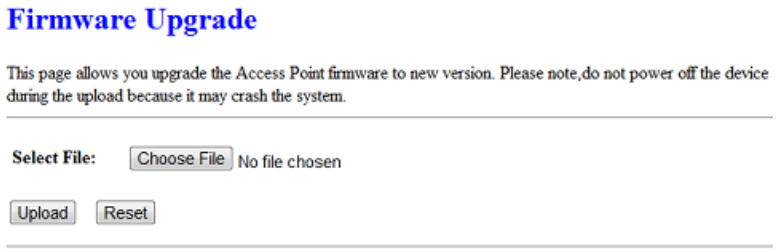

Change Password
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.
User Name:
New Password:
Confirmed Password:
Apply Change
Reset

Click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.3.3 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website

(http://www.amigo.com.tw) to see if there is any later version of firmware. Download the firmware to your computer, click Browser and point to the new firmware file. Click Upload to upgrade the firmware. You can't make any move unless the machine reboot completely.


Firmware Upgrade
This page allows you upgrade the Access Point firmware to new version. Please note,do not power off the device during the upload because it may crash the system.
Select File:
Choose File
No file chosen
Upload
Reset

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Note: The firmware upgrade will not remove your previous settings.

λ Reset button:

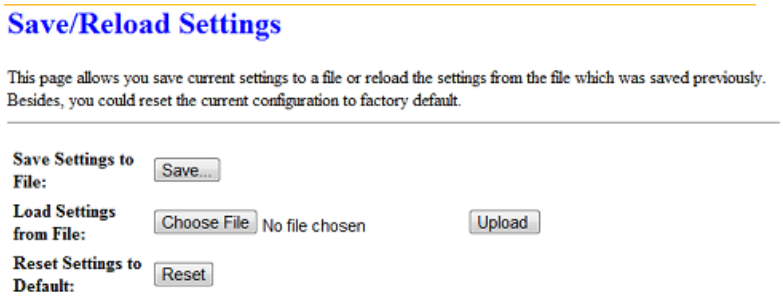
On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.

6.3.4 Profile Save

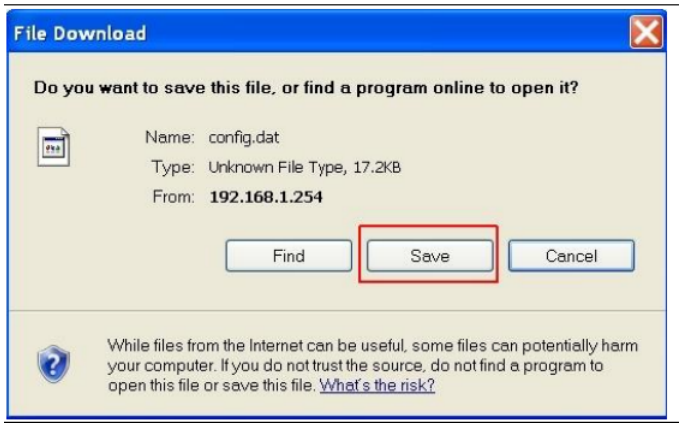
Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

1. Save Configuration

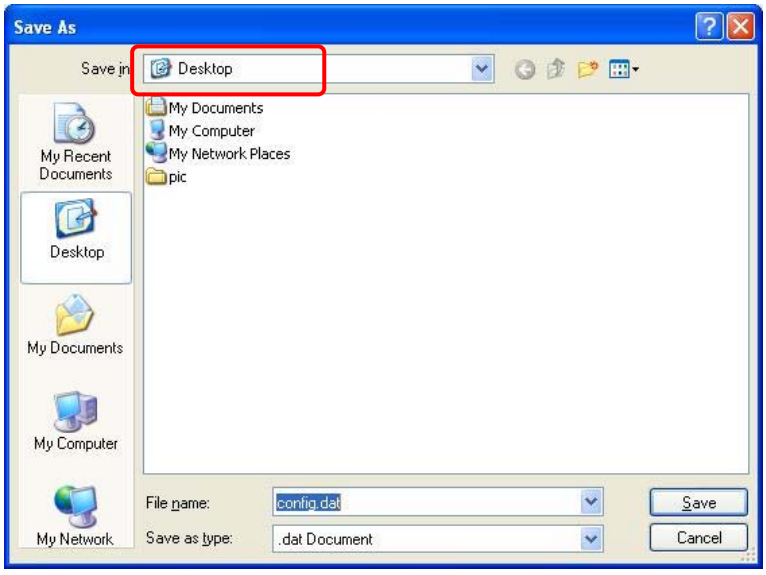
(1). Click Save


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Choose File
No file chosen
Upload
Reset Settings to Default:
Reset

(2). Please click “Save” to save the configuration to your computer.

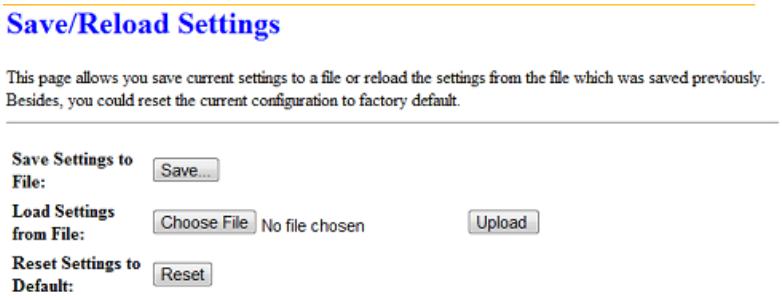

File Download
Do you want to save this file, or find a program online to open it?
Name: config.dat
Type: Unknown File Type, 17.2KB
From: 192.168.1.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

(3). Select the location which you want to save file, then click Save.

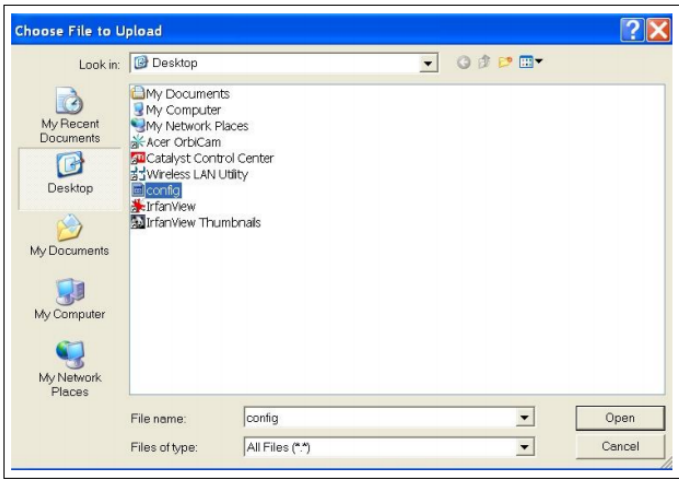


2. Load configuration file

(1). Click Choose File


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Choose File
No file chosen
Upload
Reset Settings to Default:
Reset

(2). Select configuration file then click Open



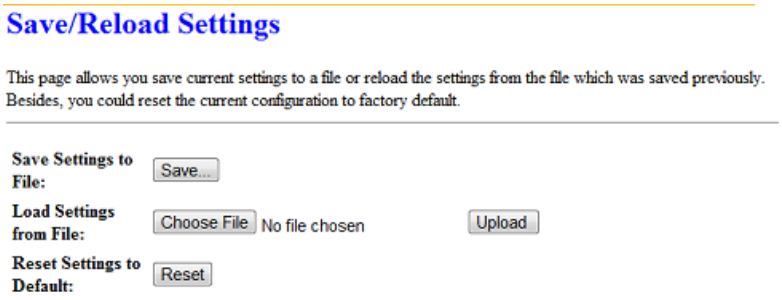
(3). Click Upload to upload configuration file to GR-1736.

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Choose File
config.dat
Upload
Reset Settings to Default:
Reset

(4). After 90 seconds, GR-1736 will reboot automatically.

3. Reload factory default setting

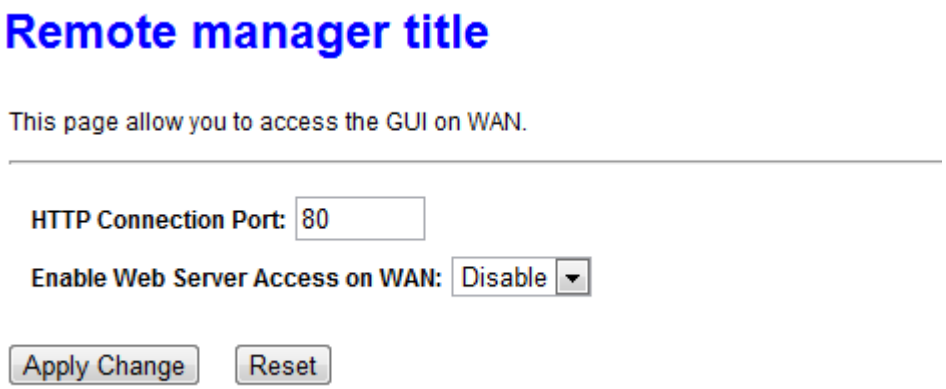
(1). Please click Reset


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously.
Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Choose File
No file chosen
Upload
Reset Settings to Default:
Reset

(2). Please click OK to start reload factory default setting to GR-1736.

(3). After 90 seconds, GR-1736 will reboot automatically.

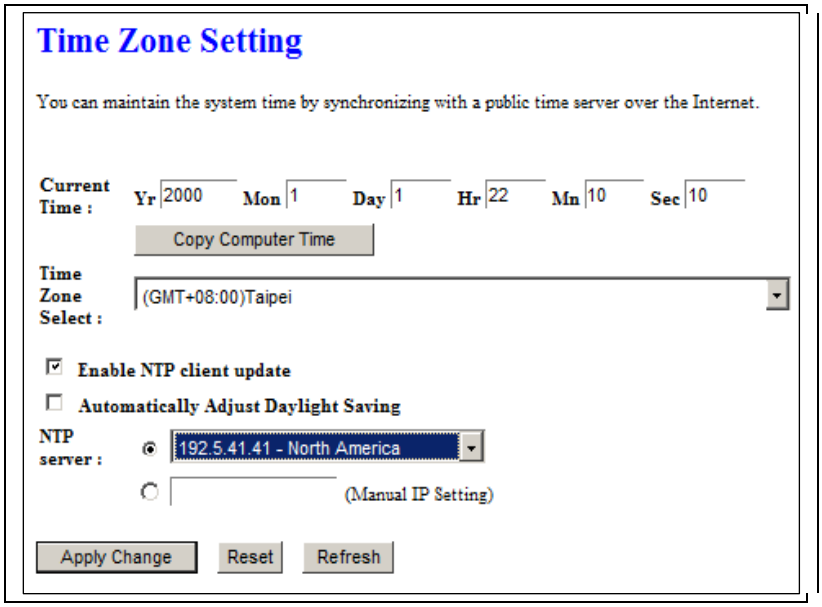
6.3.5 Remote Manager


Remote manager title
This page allow you to access the GUI on WAN.
HTTP Connection Port: 80
Enable Web Server Access on WAN: Disable
Apply Change
Reset

Item	Description
HTTP Connection Port	Users can access GUI by this port，default is 80
Enable Web Server Access on WAN	Allow user access GUI from WAN side

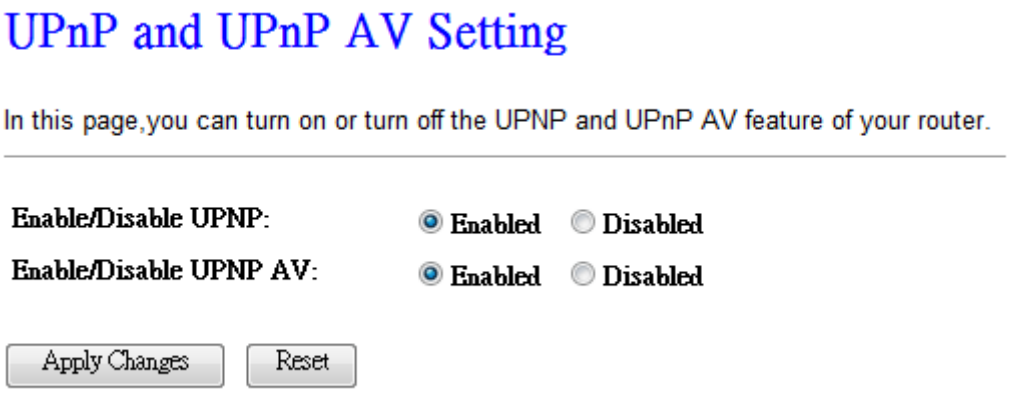
6.3.6 Time Zone Setting

Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2000 Mon 1 Day 1 Hr 22 Mn 10 Sec 10
Copy Computer Time
Time Zone Select :
(GMT+08:00)Taipei
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable Automatically Adjust Daylight Saving or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data. Or you may click on Refresh to update the system time on the screen.

6.3.7 UPnP Setting



- **UPNP**

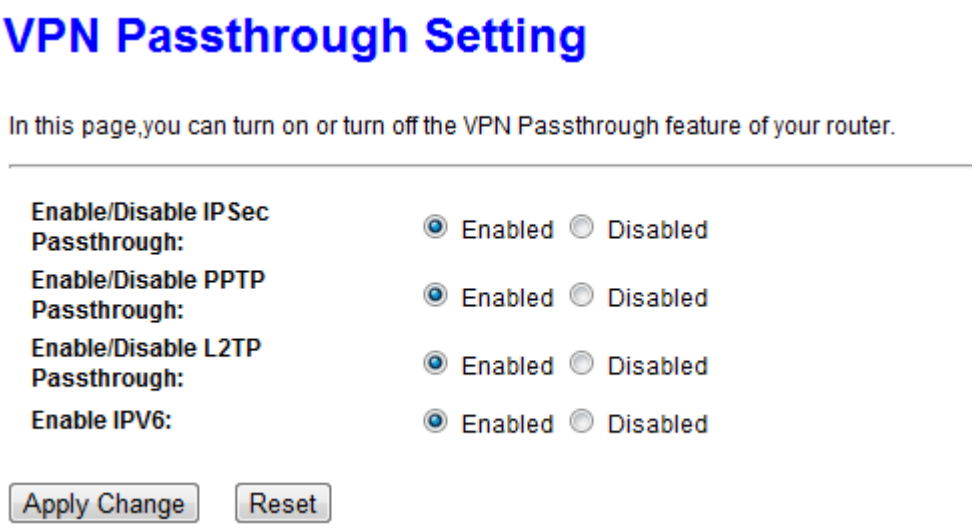
Universal Plug and Play (UPnP) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. GR-1736 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click My Network Places. Users will see an Internet Gateway Device icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

- **UPNP AV**

A UPnP AV media server is the UPnP-server that provides media library information and streams media-data (like audio/video/picture/files) to UPnP-clients on the network. It is a computer system or a similar digital appliance that stores digital media, such as photographs, movies, or music and shares these with other devices. User can plug in USB disk to product USB port and use UPnP AV client to play USB disk media-data (like audio/video/picture/files)

6.3.8 VPN Passthrough Setting

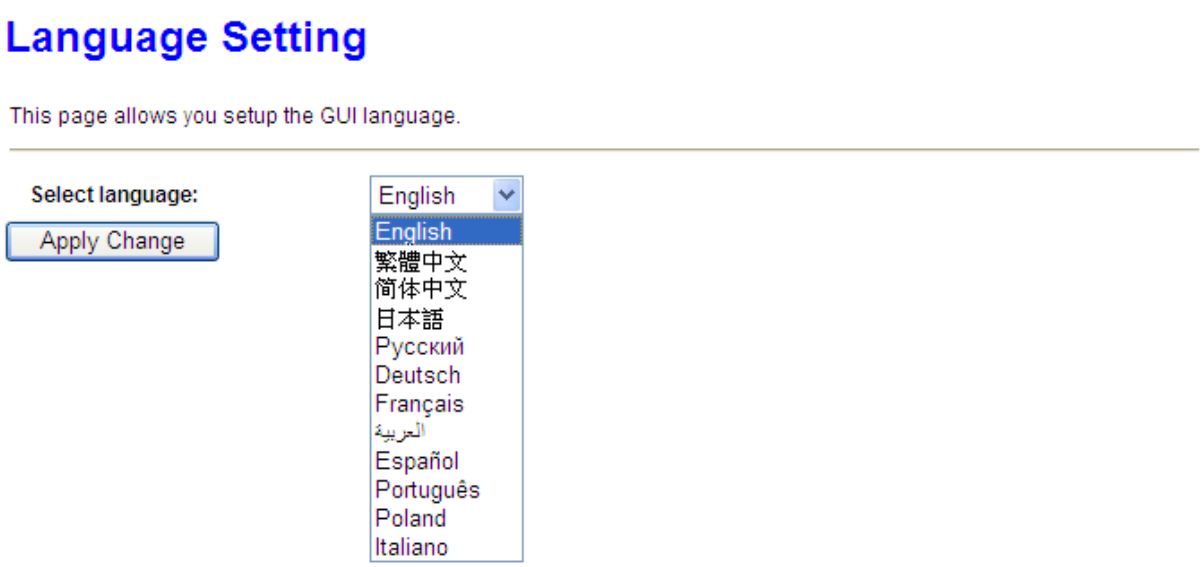
Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec, Pass-through, PPTP Pass-through, and L2TP Pass-through.



Item	Description
IPSec Pass-through	Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, IPSec Pass-through is enabled by default. To disable IPSec Pass-through , select Disable
PPTP Pass-through	Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the router, PPTP Pass-through is enabled by default. To disable PPTP Pass-through, select Disable.
L2TP Pass-through	To allow the L2TP network traffic to be forwarded to its destination without the network address translation tasks.
IPV6 Pass-through	Allow IPV6 packet to be forwarded to its destination without the network address translation tasks.
Apply Changes & Reset & Refresh	Please click on Apply Changes to save the setting data. Or you may click on Reset to clear all the input data.

6.3.9 Language Setting

The GR-1736 provide 12 languages for Web GUI. You can select the language interface from the dropdown list and by following steps.

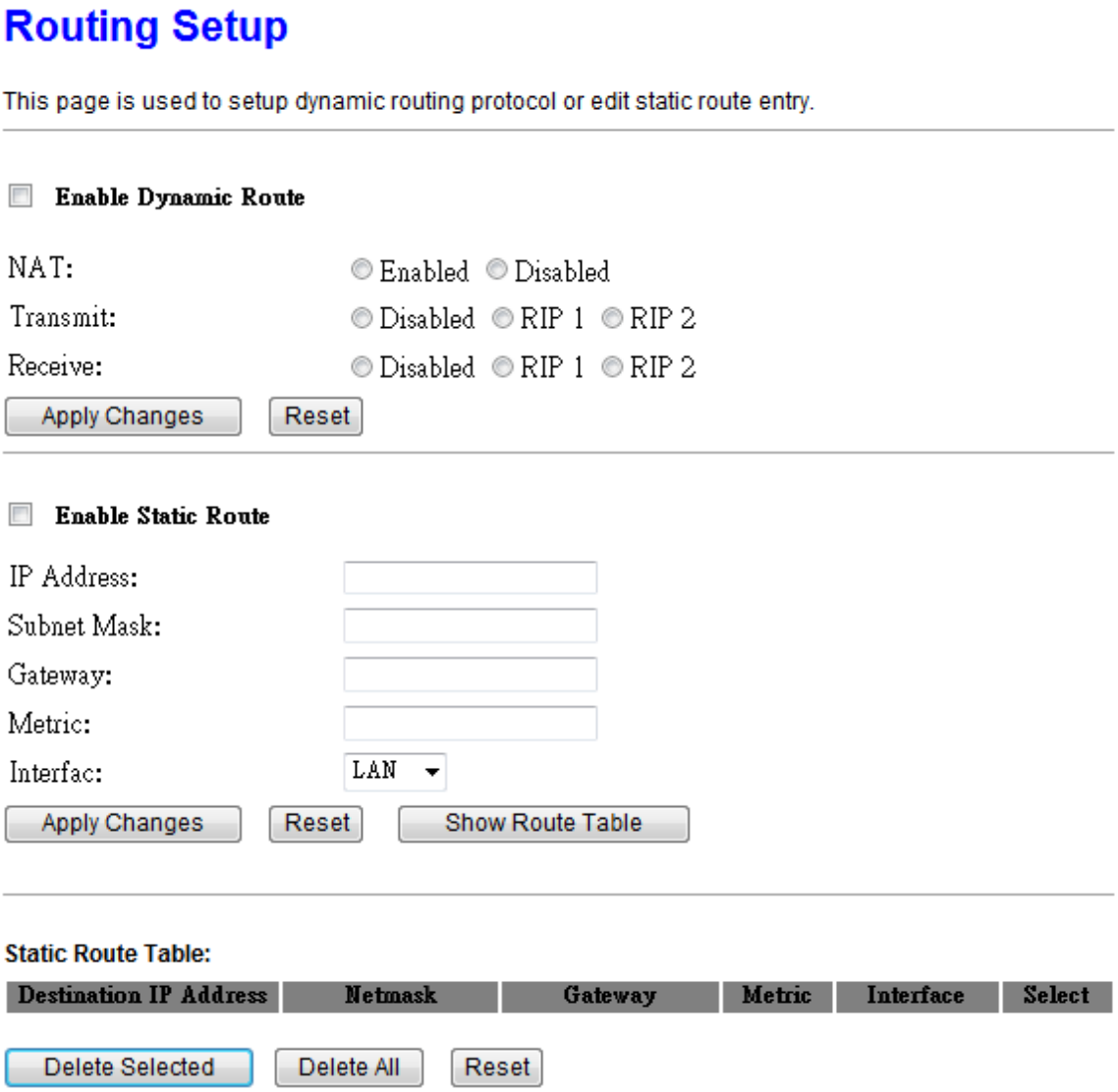


When you see the screen message change to the selected language, the setup is completed.

6.3.10 Routing Setup

Dynamic routing is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15

Static routing is a data communication concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network.This is achieved by manually adding routes to the router routing table.



Item	Description
Enable Dynamic Route	Enable or Disable dynamic route
NAT	Enable or Disable NAT function
Transmit	There are 3 options： 1. Disable：do not send any RIP packet out 2. Send RIP1 packet out 3. Send RIP2 packet out
Receive	There are 3 options： 4. Disable：do not receive any RIP packet 5. Only receive RIP1 packet 6. Only receive RIP2 packet

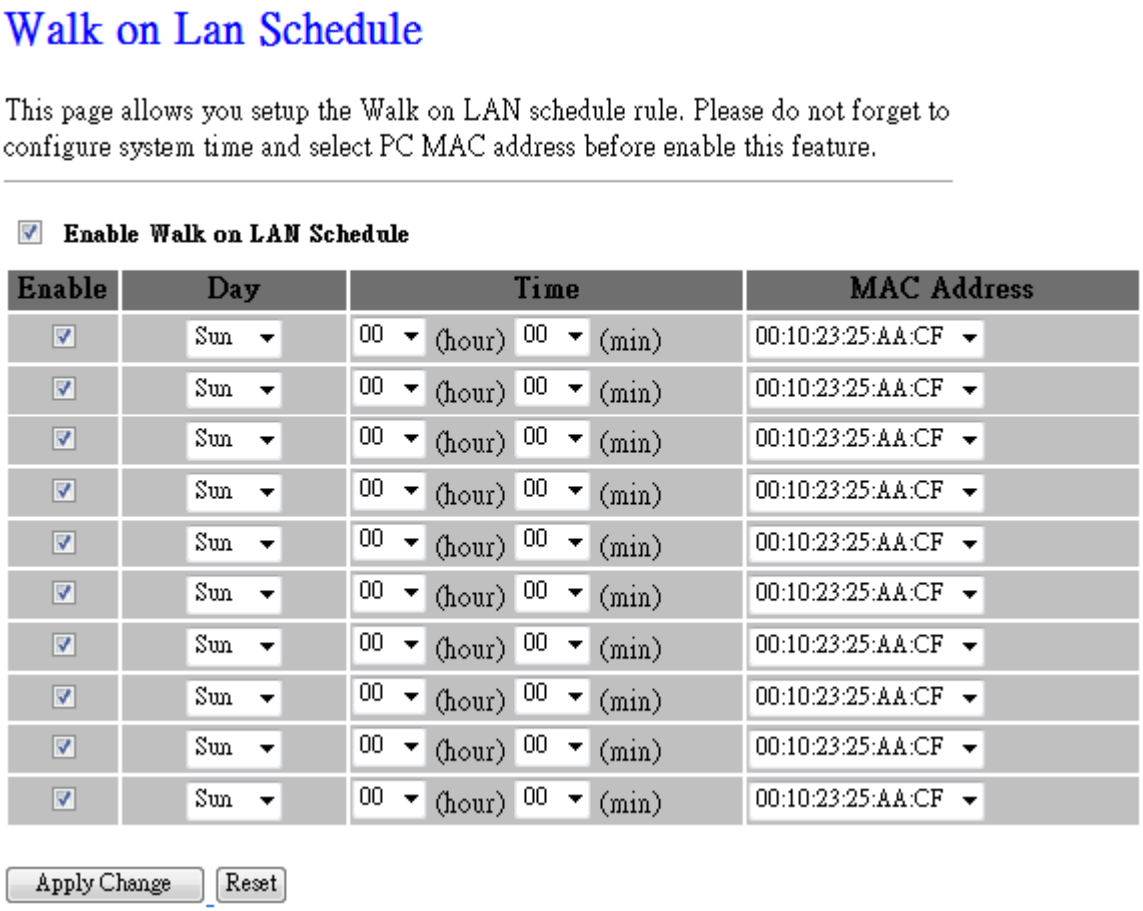
Item	Description
Enable Static Route	Enable or Disable dynamic route
IP Address	Destination IP address
Subnet Mask	Destination IP subnet mask
Gateway	Gateway IP address for destination
Metric	Metric number on router's routing table
Interface	Static route rule for LAN or WAN interface

6.3.11 User Account Settings

Set user log on locally used by the FTP server shares account, password

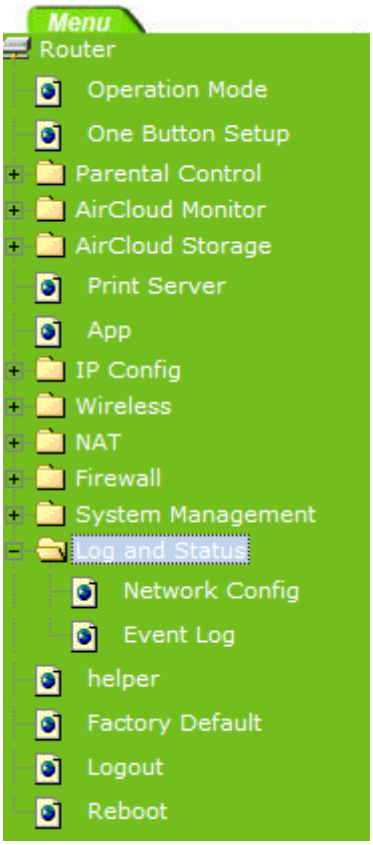
6.3.12 Walk on LAN Schedule

Switch your computer ON through your LAN or the Internet . To support WOL you must have a computer with Motherboard that supports WOL, as well as a Network Controller (NIC) supporting this function. Most of the newer Motherboard (circa 2002 and On), have an On Board NIC that supports WOL. Otherwise you need to install a PCI NIC that is WOL capable.


Walk on Lan Schedule
This page allows you setup the Walk on LAN schedule rule. Please do not forget to configure system time and select PC MAC address before enable this feature.
Enable Walk on LAN Schedule
Enable
Day
Time
MAC Address
Sun
00 (hour) 00 (min)
00:10:23:25:AA:CF
Apply Change
Reset

6.4 Log & Status

The category provides Network Config and Event Log status for users to know the operation status.



6.4.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP …information.

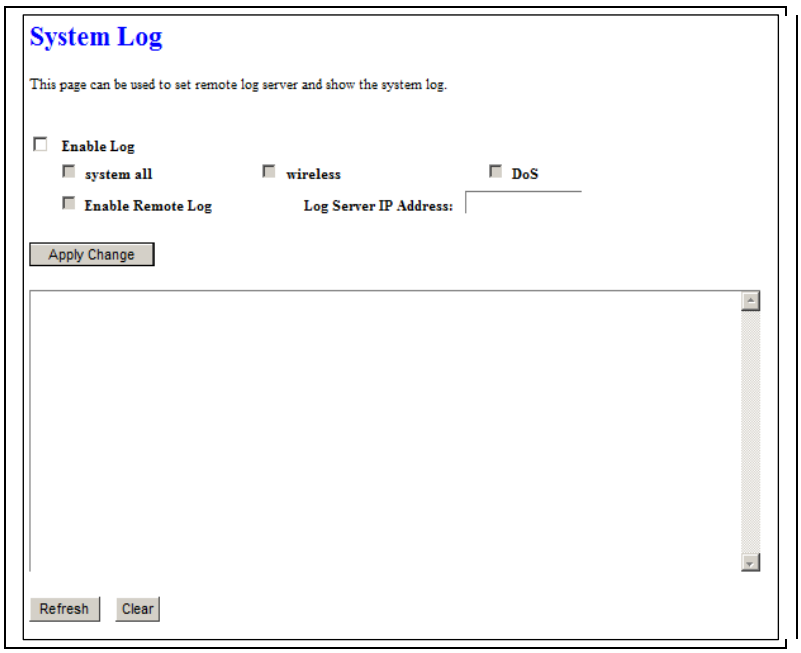
Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:33m:8s
Firmware Version	Ver1.1.42
Build Time	Wed Jan 18 11:35:43 CST 2012
Wireless 1 Configuration	
Mode	AP
Band	5 GHz (A+N)
SSID	SAPIDO_GR-1736_5G
Channel Number	44
Encryption	Disabled
MAC Address	00:e0:4c:81:98:a1
Associated Clients	0
Wireless 2 Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	SAPIDO_GR-1736_2.4G
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:98:b1
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC Address	00:e0:4c:81:98:a1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:98:a9
3.5G Configuration	
Connect Speed	Auto Switch
Signal Strength	
Network Name	
3.5G BACKUP	No

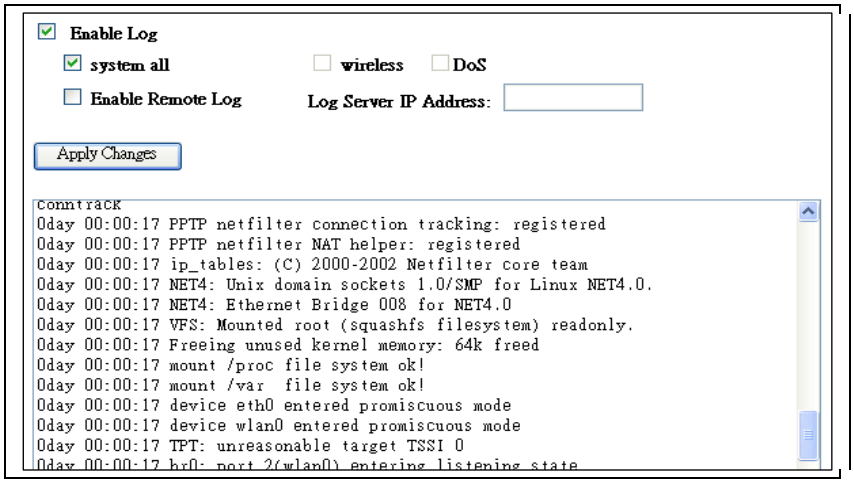
6.4.2 Event Log

You may enable the event log feature here.



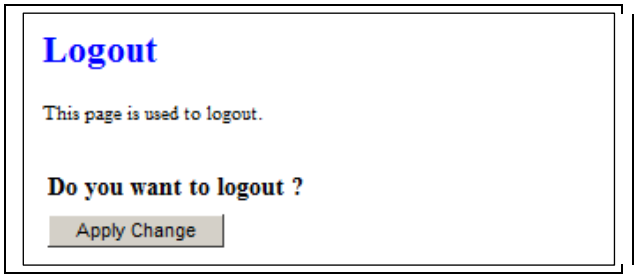
Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on Apply Changes to save the setting data. Click on Refresh to renew the system time, or on Clear to clear all the record.

* The following figure is an example when users click Apply Changes to record the event log.

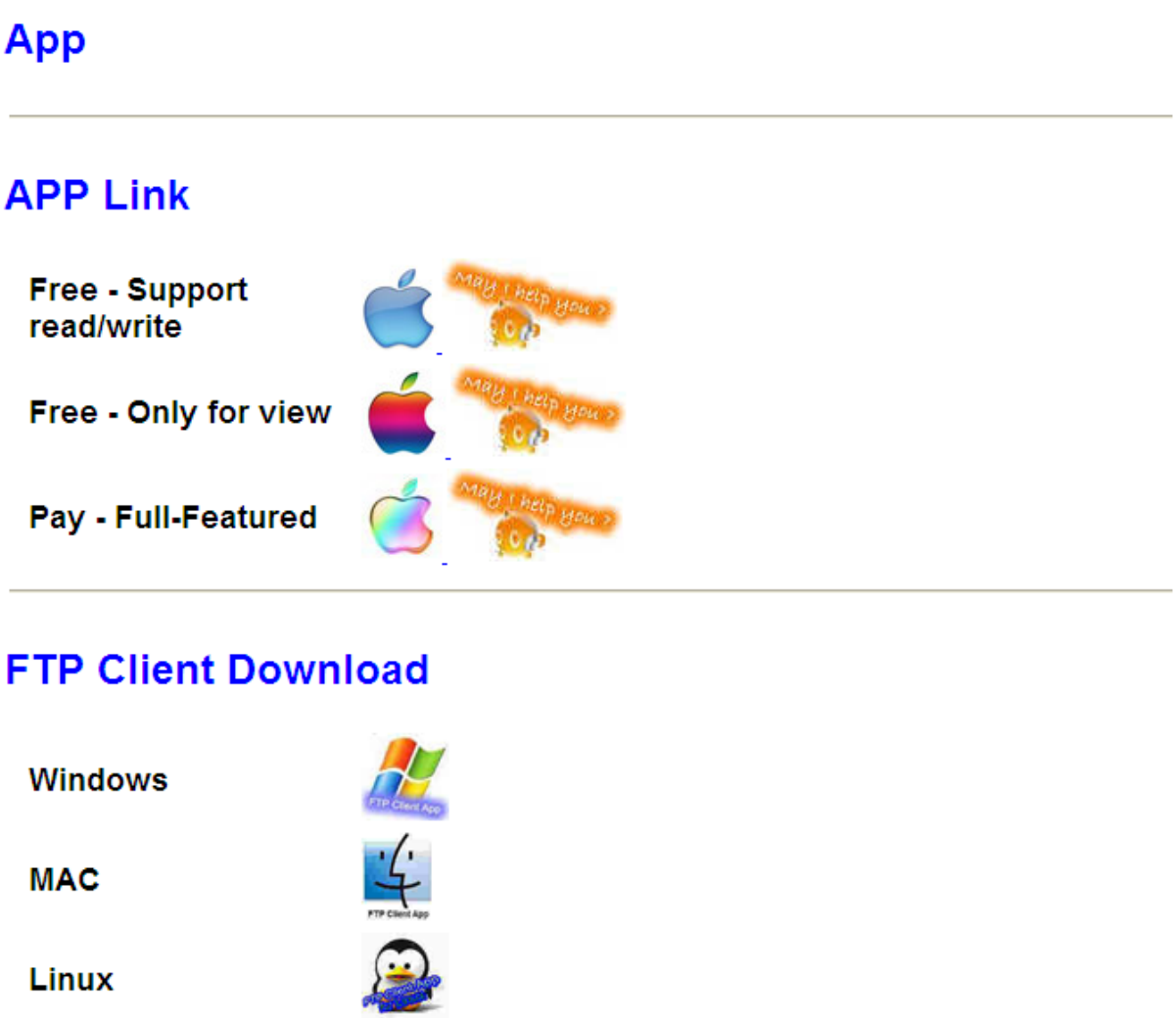

Enable Log
system all
wireless
DoS
Enable Remote Log
Log Server IP Address:
Apply Changes
Conntrack
0day 00:00:17 PPTP netfilter connection tracking: registered
0day 00:00:17 PPTP netfilter NAT helper: registered
0day 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
0day 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
0day 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
0day 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
0day 00:00:17 Freeing unused kernel memory: 64k freed
0day 00:00:17 mount /proc file system ok!
0day 00:00:17 mount /var file system ok!
0day 00:00:17 device eth0 entered promiscuous mode
0day 00:00:17 device wlan0 entered promiscuous mode
0day 00:00:17 TPT: unreasonable target TSSI 0

6.5 Logout

This function logs out the user.



6.6 App



Hyperlinks provide users quick and convenient for users to download with a third-party software on the machine

Chapter 7 Samba Server

The GR-1736 is able to act as a Samba server to share the file on USB storage in local network.

7.1 How to use GR-1736 as a Samba server

1. Plug in the USB hard disk/Flash.

2. Star your web browser and input \\192.168.1.1.

3. Star “My Computer” and you will find a folder named “sda1”.

7.2 Air play

- Connect device to router

- **Execute ipod**

7.3 Printer Server

To add an LPR port

1. Open Printers and Faxes.
2. Double-click **Add Printer** to open the Add Printer Wizard, and then click **Next**.
3. Click **Local printer attached to this computer**, clear the **Automatically detect and install my Plug and Play printer** check box, and then click **Next**.
4. Click **Create a new port**, and then click **LPR Port**.
   If **LPR Port** is not available, click **Cancel** to stop the wizard. To add the LPR port, you need to install the optional networking component, **Print Services for Unix**. For more information, click **Related Topics**.
5. Click **Next**, and then provide the following information:
   - In **Name or address of server providing LPD**, type the Domain Name System (DNS) name or Internet Protocol (IP) address of the host for the printer you are adding. The

host may be the direct-connect TCP/IP printing device or the UNIX computer to which the printing device is connected. The DNS name can be the name specified for the host in the Hosts file.

- In **Name of printer or print queue on that server**, type the name of the printer as it is identified by the host, which is either the direct-connect printer itself or the UNIX computer.

6. Follow the instructions on the screen to finish installing the TCP/IP printer.

Notes

- To open Printers and Faxes, click **Start**, and then click **Printers and Faxes**.
- The Line Printer Remote (LPR) port is best suited to servers that need to communicate with host computers (such as UNIX or VAX computers) by way of RFC 1179.
- A network-connected printer must have a card that supports LPD for LPR printing to work properly.
- You can also add ports using the **Print Server Properties** dialog box. For more information, click **Related Topics**.
- Please refer DUT/Network Config page to get name of printer

LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
MAC Address	00:e0:4c:5a:4e:87
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.166
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
MAC Address	00:e0:4c:5a:4e:8f
3.5G Configuration	
Connect Speed	Auto Switch
Signal Strength	
Network Name	
Printer Configuration	
Printer Server	Enable
Printer Name	DeskJet 940C
Printer Model	Hewlett-Packard

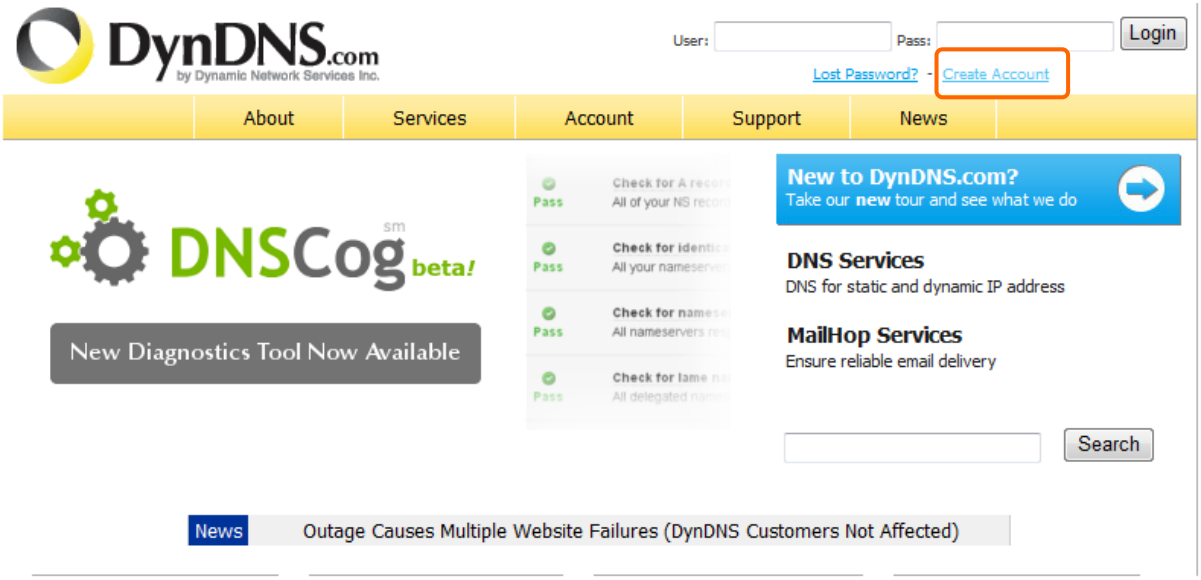
Chapter 8 DDNS Service Application

DDNS is a service changes the dynamic IP to the static IP. The settings of DDNS can solve the problem of being given the different IP by router every time. After setting the Router, your host name would correspond to your dynamic IP. Moreover, via the host name application, it could be easier for you to use FTP, Webcam and Printer remotely.

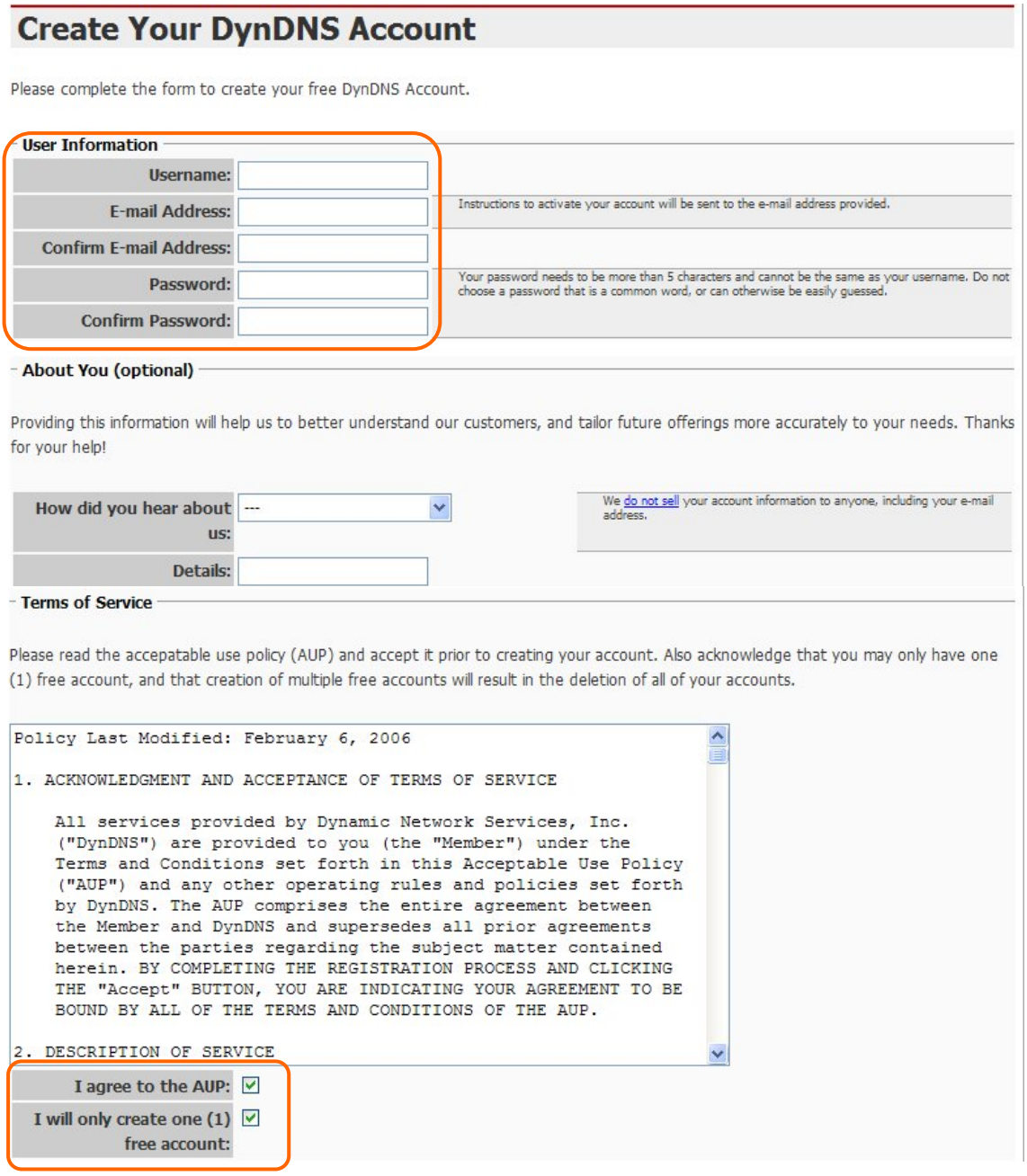
Dynamic DNS allows you to make an assumed name as a dynamic IP address to a static host name. Please configure the dynamic DNS below. Please select **Dynamic DNS** under the **IP Config** folder, and follow the instructions below to enter the **Dynamic DNS** page to configure the settings you want.

If you don't have a DDNS account, please follow the steps to complete your DDNS with Dynamic IP settings.

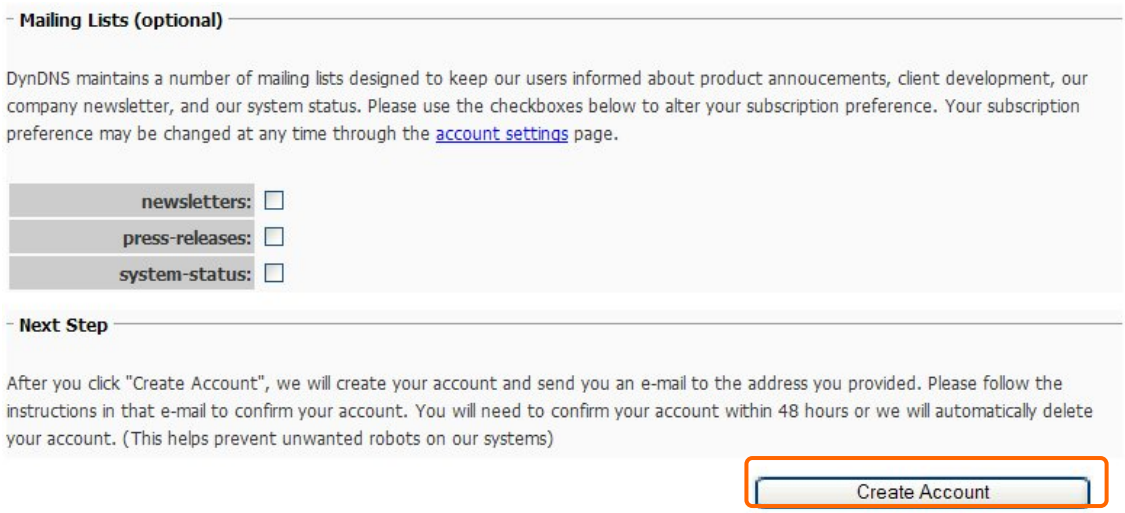
1. First access the Internet and fill http://www.dyndns.com/ into the address field of your web browser, then click **Create Account**.



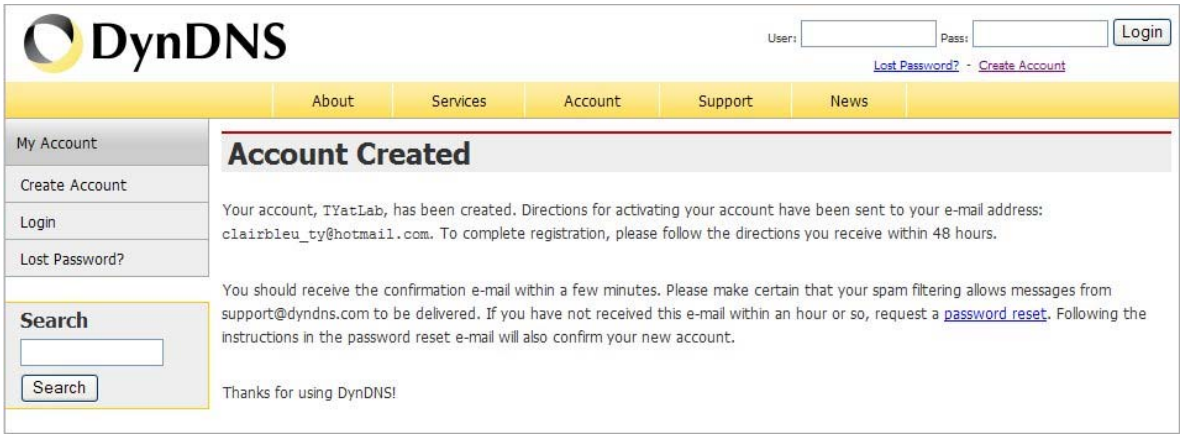
2. Fill in the form as required, and then click on **Create Account** button.


Create Your DynDNS Account
Please complete the form to create your free DynDNS Account.
User Information
Username:
E-mail Address:
Instructions to activate your account will be sent to the e-mail address provided.
Confirm E-mail Address:
Password:
Your password needs to be more than 5 characters and cannot be the same as your username. Do not choose a password that is a common word, or can otherwise be easily guessed.
Confirm Password:
About You (optional)
Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!
How did you hear about us:

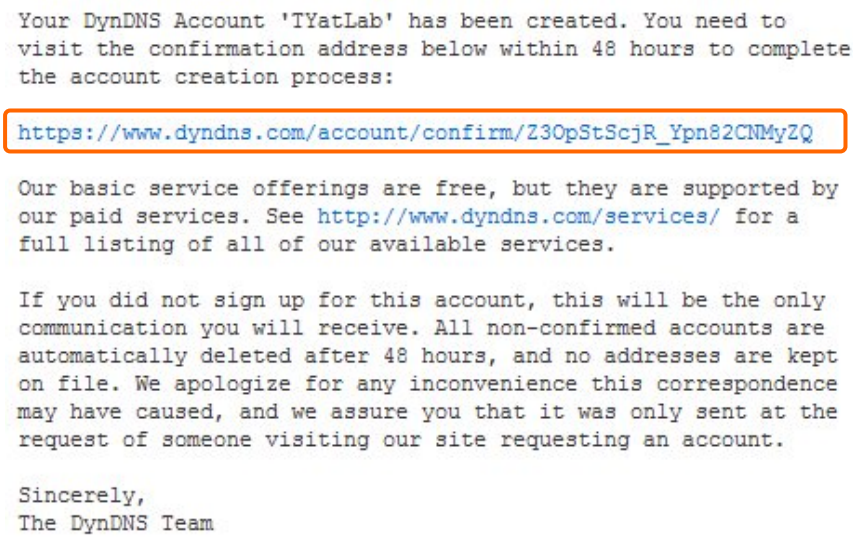
We do not sell your account information to anyone, including your e-mail address.
Details:
Terms of Service
Please read the accepatable use policy (AUP) and accept it prior to creating your account. Also acknowledge that you may only have one (1) free account, and that creation of multiple free accounts will result in the deletion of all of your accounts.
Policy Last Modified: February 6, 2006
1. ACKNOWLEDGMENT AND ACCEPTANCE OF TERMS OF SERVICE
All services provided by Dynamic Network Services, Inc. ("DynDNS") are provided to you (the "Member") under the Terms and Conditions set forth in this Acceptable Use Policy ("AUP") and any other operating rules and policies set forth by DynDNS. The AUP comprises the entire agreement between the Member and DynDNS and supersedes all prior agreements between the parties regarding the subject matter contained herein. BY COMPLETING THE REGISTRATION PROCESS AND CLICKING THE "Accept" BUTTON, YOU ARE INDICATING YOUR AGREEMENT TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THE AUP.
2. DESCRIPTION OF SERVICE
I agree to the AUP:
I will only create one (1) free account:


Mailing Lists (optional)
DynDNS maintains a number of mailing lists designed to keep our users informed about product annoucements, client development, our company newsletter, and our system status. Please use the checkboxes below to alter your subscription preference. Your subscription preference may be changed at any time through the account settings page.
newsletters:
press-releases:
system-status:
Next Step
After you click "Create Account", we will create your account and send you an e-mail to the address you provided. Please follow the instructions in that e-mail to confirm your account. You will need to confirm your account within 48 hours or we will automatically delete your account. (This helps prevent unwanted robots on our systems)
Create Account

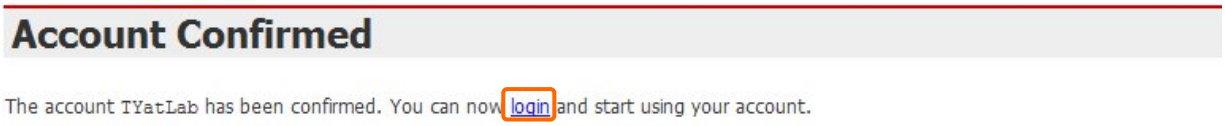
3. When you got this account created message, close it, and check your mailbox. You would get a mail from DynDNS website.


DynDNS
User:
Pass:
Login
Lost Password? - Create Account
About
Services
Account
Support
News
My Account
Create Account
Login
Lost Password?
Search
Search
Account Created
Your account, TYatLab, has been created. Directions for activating your account have been sent to your e-mail address: clairbleu_ty@hotmail.com. To complete registration, please follow the directions you receive within 48 hours.
You should receive the confirmation e-mail within a few minutes. Please make certain that your spam filtering allows messages from support@dyndns.com to be delivered. If you have not received this e-mail within an hour or so, request a password reset. Following the instructions in the password reset e-mail will also confirm your new account.
Thanks for using DynDNS!

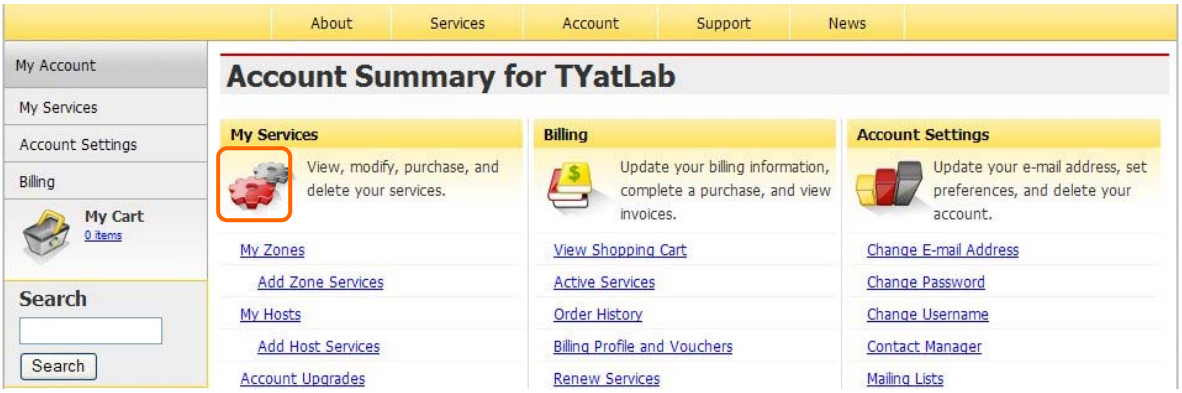
4. Click on the indicated address within your mail to confirm.


Your DynDNS Account 'TYatLab' has been created. You need to visit the confirmation address below within 48 hours to complete the account creation process:
https://www.dyndns.com/account/confirm/Z3OpStScjR_Ypn82CNMyZQ
Our basic service offerings are free, but they are supported by our paid services. See http://www.dyndns.com/services/ for a full listing of all of our available services.
If you did not sign up for this account, this will be the only communication you will receive. All non-confirmed accounts are automatically deleted after 48 hours, and no addresses are kept on file. We apologize for any inconvenience this correspondence may have caused, and we assure you that it was only sent at the request of someone visiting our site requesting an account.
Sincerely,
The DynDNS Team

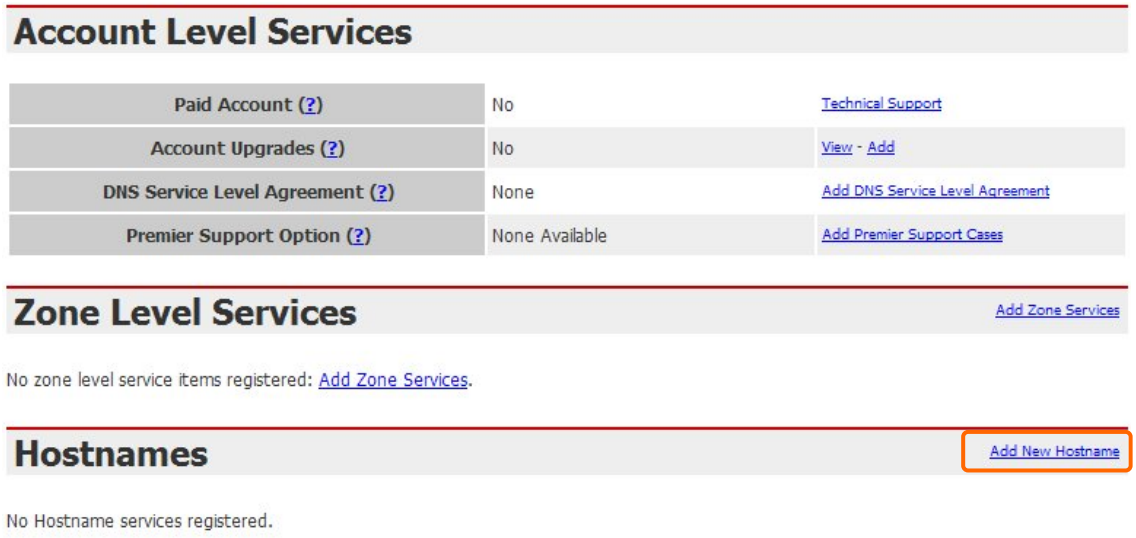
5. Click on **login.**


Account Confirmed
The account TYatLab has been confirmed. You can now login and start using your account.
Be informed of new services, changes to services, and important system maintenance/status notifications by subscribing to our mailing lists.
Once there, you may susbscribe to the Announce list by checking the appropriate box and clicking the "Save Settings" button.

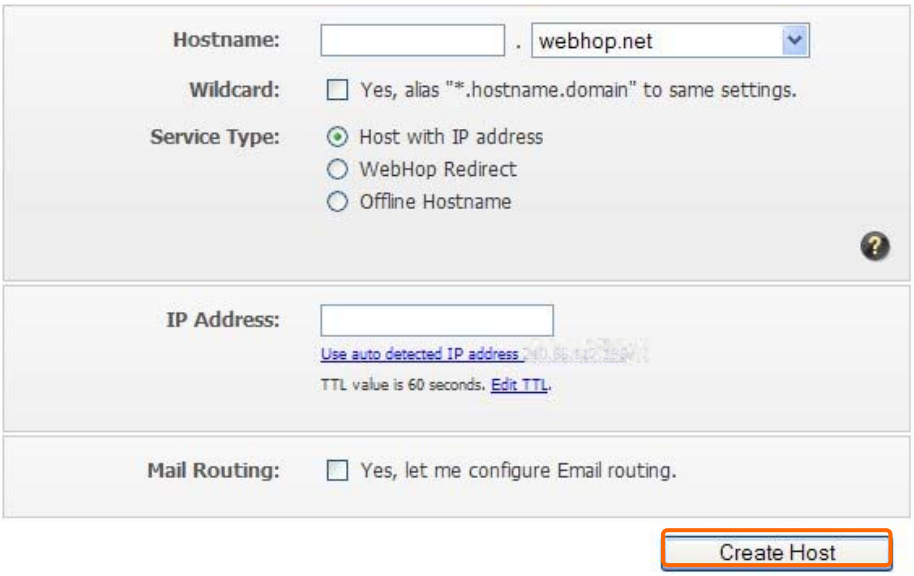
6. Click **My Services** after logging in.



7. Click **Add New Hostname**.


Account Level Services
Paid Account (?) No Technical Support
Account Upgrades (?) No View - Add
DNS Service Level Agreement (?) None Add DNS Service Level Agreement
Premier Support Option (?) None Available Add Premier Support Cases
Zone Level Services
Add Zone Services
No zone level service items registered: Add Zone Services.
Hostnames
Add New Hostname
No Hostname services registered.

8. Put in your favorite hostname and service type, and then click **Create Host** after finished.



9. Your hostname has been created when you see the following page.

Chapter 9 Q & A

9.1 Installation

1. Q: Where is the XDSL Router installed on the network?

A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. Q: Why does the throughput seem slow?

A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the network does not exceed 10 broadcast messages per second.
- Verify network topology and configuration.

9.2 LED

1. Why doesn't GR-1736 power up?

A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. The Internet browser still cannot find or connect to GR-1736 after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.

A: In case GR-1736 is inaccessible; you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 7 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. Why does GR-1736 shut down unexpectedly?

A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

9.3 IP Address

1. **Q: What is the default IP address of the router for LAN port?**

   A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. **Q: I don't know my WAN IP.**

   A: There are two ways to know.

   Way 1: Check with your Internet Service Provider.

   Way 2: Check the setting screen of GR-1736. Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. **How can I check whether I have static WAN IP Address?**

   A: Consult your ISP to confirm the information, or check Network Configuration in GR-1736 ’s Main Menu.

4. **Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?**

   A: Yes, the Router mode allows for customization of your public IPs and Domain.

9.4 OS Setting

1. **Why can’t my computer work online after connecting to GR-1736?**

   A: It’s possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start**＞**Settings**＞ **Network and Dial-up Connections**＞double click on **Internet Protocol(TCP/IP)**＞ select **obtain IP address automatically**＞ Click on **OK** button. Then, open Internet browser for testing. If you still can’t go online, please test something else below.

   - Verify network configuration by ensuring that there are no duplicate IP addresses.
   - Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.
   - Check that the cables and connectors or use another LAN cable.

2. **Q: Why can't I connect to the router's configuration utility?**

A: Possible Solution 1: Make sure that your Ethernet connect properly and securely. Make sure that you've plugged in the power cord.

Possible Solution 2: Make sure that your PC is using an IP address within the range of 192.168.1.2 to 192.168.1.254. Make sure that the address of the subnet mask is 255.255.255.0. If necessary, the Default Gateway data should be at 192.168.1.1. To verify these settings, perform the following steps:

Windows 2000, or XP Users:

1. Click on Windows **Start** > click on **Run** > input **cmd** > click on **OK** button.
2. At the DOS prompt, type ipconfig/all.
3. Check the IP Address, Subnet Mask, Default Gateway data. Is this data correct? If the data isn't correct. Please input **ipconfig/release** > press **Enter** > input **ipconfig/renew** > press **Enter**.

Possible Solution 3: Verify the connection setting of your Web browser and verify that the HTTP Proxy feature of your Web browser is disabled. Make these verifications so that your Web browser can read configuration pages inside your router. Launch your Web browser.

Internet Explorer Users:

1. Click on **Tools** > **Internet Options** > **Connections tab**.
2. Select **never dial a connection**, click on **Apply** button, and then click on **OK** button.
3. Click on **Tools** and then click on **Internet Options**.
4. Click on **Connections** and then click on **LAN Settings**.
5. Make sure none of the check boxes are selected and click on **OK** button.
6. Click on OK button.

Netscape Navigator Users:

1. Click on **Edit** > **Preferences** > double-click **Advanced** in the Category window.
2. Click on **Proxies** > select **Direct connection to the Internet** > click on **OK** button.
3. Click on **Edit again** and then click on **Preferences**.
4. Under category, double-click on **Advanced** and then click on **Proxies**.
5. Select **Direct connection to the Internet** and click on **OK** button.
6. Click on **OK** button.

3. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

4. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

9.5 GR-1736 Setup

1. Q: Why does GR-1736's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in GR-1736 's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via GR-1736. Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server under** the **IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

3. Q: How do I upgrade the firmware of GR-1736 ?

A: Periodically, a new Flash Code is available for GR-1736 on your product supplier's website. Ideally, you should update GR-1736's Flash Code using **Firmware Upgrade** on the **System Management** menu of GR-1736 Settings.

4. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

5. Q: GR-1736 couldn't save the setting after click on Apply button?

A: GR-1736 will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboot** under **System Management** directory**.**

9.6 Wireless LAN

1. Q: Why couldn’t my wireless notebook work on-line after checking?

A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. Q: My PC can't locate the Wireless Access Point.

A: Check the following:

- Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. Q: Wireless connection speed is very slow.

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. Q: Some applications do not run properly when using the Wireless Router.

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. Q: I can't connect to the Wireless Router to configure it.

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. Q: The WinXP wireless interface couldn't communicate the WEP with GR-1736's wireless interface.

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of GR-1736 is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and GR-1736 would be communicated.

9.7 Support

1. Q: What is the maximum number of IP addresses that the XDSL Router will support?

A: The Router will support to 253 IP addresses with NAT mode.

5. Q: Is the Router cross-platform compatible?

A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

9.8 Others

1. Q: Why does the router dial out for PPPoE mode very often?

A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

2. Q: What can I do if there is already a DHCP server in LAN?

A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.

9.9 USB Device

1. Q: How many USB devices can be connected to the Product?

A: GR-1736 has 2 USB ports.

Chapter 10 Appendices

10.1 Operating Systems

1. Microsoft：Windows 2000, XP, Vista, Windows 7.
2. Apple：Mac OS X 10.4.7, Leopard and the following related versions.
3. Linux：Redhat 9, Fedora 6 & 7, Ubuntu 7.04 and the following related versions.

10.2 Browsers

1. Internet Explorer ver. 6 and 7 and the following related versions.
2. FireFox ver. 2.0.0.11 and the following related versions.3.
3. Safari ver. 3.04 and the following related versions.

10.3 Communications Regulation Information

Should any consumers need to learn more information, services and supports, please contact the supplier of your product directly.